Volume 106
Issue 2 *Dickinson Law Review - Volume 106, 2001-2002*

10-1-2001

CyberLaw: A Brave New World

Richard A. Mann

Barry S. Roberts

CyberLaw: A Brave New World

Richard A. Mann* and Barry S. Roberts**

Technology and business have frequently outpaced the law. In today's business environment, the widening of this gap has accelerated with the rapid growth of e-commerce and communication on the Internet.[1] The resulting legal vacuum has not only created considerable uncertainty in business transactions, but also created numerous opportunities for abuse. In this article we will identify some of the types of legal and regulatory issues that have arisen or are likely to arise. We will also describe the extent to which the law has responded or is in the process of responding. This article will cover the following areas of the law that have been most significantly affected by e-commerce and the evolution of the Internet: defamation, intellectual property, contract and sales law, privacy, securities regulation, and cyber crime.

I. Defamation

A. The Elements

Defamation, whether in the "real" world or in "cyberspace," occurs when a false statement harms the reputation of another.[2] In

* Professor of Business Law, Kenan-Flagler Business School, University of North Carolina, B.S. University of North Carolina, J.D. Yale Law School.

** Professor of Business Law, Kenan-Flagler Business School, University of North Carolina, B.S. Pennsylvania State University, J.D. University of Pennsylvania School of Law, LL.M. Harvard Law School. The authors thank our research assistant Michael O'Sullivan for his invaluable help on this project.

1. For example, between 1995 and 2000 the number of people online quintupled. http://www.commerce.net/research/stats/wwwpop.html (last visited May 10, 2001); http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_594751,00.html (last visited May 10, 2001).

2. *See* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 111, at 773-74 (5th ed. 1984) (discussing the varying definitions of defamation among different jurisdictions). *See id.* at 774-78 (providing examples of defamatory statements and the circumstances surrounding a particular statement that may make it defamatory).

most jurisdictions, the elements of a defamation action include the following: (1) a false and defamatory statement concerning another person, and (2) an unprivileged publication (communication) to a third party. Additionally, in some cases, depending on the "public" or private status of the victim, a third element is required: some degree of fault on her part in knowing or failing to ascertain the falsity of the statement. Furthermore, in some cases, a fourth element is required: proof of special harm caused by the publication. Defamatory means causing injury to a person's reputation by disgracing her and diminishing the respect within which she is held.[3] An example of a defamatory injury is publishing a false statement that a person had committed a crime or had committed an offensive act. The plaintiff bears the burden of proof in a defamation action to prove the falsity of the statement. To date, defamation by way of the Internet has been treated as libel[4] rather than as slander,[5] similar to the treatment of defamation by way of radio and television.

One defamation issue, in both traditional media and cyberspace, is the classification of a party as a publisher or distributor.[6] The distinction is key because a publisher, upon a showing of the appropriate level of fault,[7] may be held liable for a defamatory statement, while a distributor may be held liable only if it is shown that he knew or had reason to know of the defamatory statement.[8] Typically, the author is a publisher, as well as any other party that exercised editorial control over the writing of the piece or whose business it is to disseminate the piece.[9] The most common examples of the latter are newspapers, book publishers and

3. *See* RESTATEMENT (SECOND) OF TORTS (hereinafter RESTATEMENT) § 558 (1977). *See generally* Lyrissa Barnett Lidsky, *Article: Defamation, Reputation, and the Myth of Community*, 71 WASH. L. REV. 1 (1996) (evaluating the effectiveness of the community standard when courts determine whether a statement is defamatory).

4. Libel is generally written. *See* KEETON ET AL., *supra* note 2, at 771.

5. Slander is usually oral. *See id. But see* Sheri Hunter, *Defamation and Privacy Laws Face the Internet*, 17 COMM. LAW. 16, n.1 (1999) (noting that further technological advances may make slander a viable tort on the Internet).

6. The term distributor carries the same meaning as a secondary publisher or secondary disseminator. *See* KEETON ET AL., *supra* note 2, at 803.

7. *See, e.g.*, Gertz v. Welch, 418 U.S. 323, 342 (1974) (differentiating between the actual malice requirement for public officials in New York Times Co. v. Sullivan, 376 U.S. 254 (1964), later extended to public officials in Curtis Publ'g Co. v. Butts, 388 U.S. 130 (1967), and a lesser standard for private persons).

8. *Compare* KEETON ET AL., *supra* note 2, at 811, *with* RESTATEMENT, *supra* note 3, § 612, cmt. e (discussing the limits of a distributor's privilege to publish known defamatory statements).

9. *See* KEETON ET AL., *supra* note 2, at 803, 810.

television stations.[10] By contrast, those who do not participate in the writing or editing of a defamatory statement but merely assist in its distribution are considered distributors rather than publishers.[11] Libraries, newsstands, book stores and even paperboys are examples of distributors.[12]

B. Early Cases Involving ISP Liability

The first Internet defamation cases, *Cubby, Inc. v. CompuServe Inc.* and *Stratton Oakmont, Inc. v. Prodigy Services Co.*, focused on the liability of Internet Service Providers ("ISPs"). In 1990, plaintiffs claimed they were defamed in an online newsletter known as *Journalism Forum* and sued CompuServe in New York.[13] CompuServe provided *Journalism Forum* to its Internet users through a contract with Cameron Communications Inc., a company that agreed to exercise editorial control over the *Journalism Forum*.[14] However, CompuServe did not review *Journalism Forum*'s material before distributing the newsletter to Internet users.[15] As a result, the court held that CompuServe was not liable because it distributed *Journalism Forum* without knowledge of its allegedly defamatory statements.[16]

Several years later, another New York court addressed the issue of ISP liability. A securities firm sued Prodigy, claiming it was defamed after an anonymous user posted statements that the firm's employees had engaged in fraud and were paid to lie.[17] The court held that Prodigy acted as the publisher of an online financial bulletin board.[18] In distinguishing Prodigy from CompuServe, the court found that Prodigy had held itself out as a family-oriented site that exercised editorial control over posted messages.[19] The court

---

10. *See id.* at 803.
11. *See id.* at 803-04, 810-11.
12. *See id.* at 803.
13. Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
14. *See id.* at 137.
15. *See id.* In addition, CompuServe did not enter into a contract with the party providing the defamatory information appearing on the *Journalism Forum*.
16. *See id.* at 139 (citing Smith v. California, 361 U.S. 147 (1959), where the Supreme Court struck down a state statute making it a crime for a shop owner to distribute materials that he had not reviewed). "Every bookseller would be placed under an obligation to make himself aware of the contents of every book in his shop. It would be altogether unreasonable to demand so . . . ." *Id.* (quoting *Smith*, 361 U.S. at 153).
17. *See* Stratton Oakmont, Inc. v. Prodigy Services Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).
18. *Id.*
19. *See id.* at *5 (finding that Prodigy advertised that it controlled content, and

compared Prodigy's editorial actions to those of a newspaper publisher and concluded that Prodigy was liable to the plaintiff because it acted as a publisher.[20]

C. *Congress's Reaction: The Communications Decency Act of 1996*

In response to the *Stratton* decision, Congress passed section 230 of the Communications Decency Act of 1996 ("CDA").[21] Essentially reinstating the *Cubby* decision, this provision grants ISPs immunity when publishing information originating from a third party.[22] The language of section 230 provides, in part, that "[n]o provider ... shall be treated as the publisher ... of any information provided by another information content provider."[23] A literal interpretation of this language is that Congress intended that ISPs could be liable as distributors where it is shown they knew or should have known of the defamatory content.[24]

The CDA was first interpreted in *Zeran v. American Online, Inc.*[25] In 1995, a posting was made on an American Online, Inc ("AOL") bulletin board stating that the plaintiff, Kenneth Zeran, was selling t-shirts that depicted "offensive and tasteless slogans" regarding the Oklahoma City Federal Building bombing.[26] The posting instructed potential purchasers to call the plaintiff,

---

that its software and employees screened posted messages).

20. *See id.* at *3 (citing Miami Herald Publishing Co. v. Tornillo, 418 U.S. 241, 258 (1974) (holding that editorial decisions for newspaper publications heighten the newspaper's liability for that content)).

21. Pub. L. No. 104-104, 110 Stat. 56 (codified as amended at 47 U.S.C. § 230 (1996)). *See* Barry J. Waldman, *A Unified Approach to Cyber-libel: Defamation on the Internet, a Suggested Approach*, 6 RICH. J.L. & TECH. 9 (1999) *at* http://www.richmond.edu /jolt/v6i2/note1.html (last visited May 10, 2001).

22. Though much of the CDA was later found unconstitutional, Section 230 remains in force. *See* Reno v. ACLU, 521 U.S. 844 (1997) (holding that parts of the CDA aimed at protecting minors from pornography violated free speech rights embodied in the First Amendment).

23. 47 U.S.C. § 230(c)(1) (1996). An information content provider is defined by the CDA as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." *See id.* § 230(f)(3).

24. *See* Waldman, *supra* note 21. *See generally* KEETON ET AL., *supra* note 2, at 803-04, 810-11 (discussing classifications as primary publishers or secondary publishers (distributors) and the corresponding levels of liability for each classification). *See also* Robert M. O'Neil, *The Drudge Case: A Look at Issues in Cyberspace Defamation*, 73 WASH. L. REV. 623, 627-29 (1998) (analyzing the publisher/distributor classification in cyberspace).

25. 129 F.3d 327 (4th Cir. 1997).

26. *See id.* at 329.

providing the plaintiff's name and home telephone number on the t-shirts.[27] Mr. Zeran sued AOL (1) for failing to remove the posting after he gave the company notification and (2) because AOL did not post a retraction.[28] The court adopted a broad reading of the ISP immunity granted by the CDA holding that immunity extended to ISPs regardless of their classifications as either publishers or distributors.[29]

Critics of the *Zeran* decision argue that the court's interpretation negated the primary purpose of section 230, which was to encourage ISPs to continue to content-monitor their sites.[30] Before Congress passed the CDA, the *Stratton* decision provided a disincentive for ISPs to content-monitor. With the enactment of the CDA, section 230, also known as the "Good Samaritan Provision," guaranteed immunity for those ISPs who voluntarily, and in "good faith," blocked or screened offensive material.[31] But by eliminating any possible liability for ISPs, even as distributors with knowledge of the defamatory posting, the court has again created a disincentive for ISPs to content-monitor.[32]

---

27. *See id.*

28. *See id.* at 329-30.

29. If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. Thus liability upon notice has a chilling effect on the freedom of Internet speech.

Similarly, notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services. Any efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability. Instead of subjecting themselves to further possible lawsuits, service providers would likely eschew any attempts at self-regulation. (citations omitted.) *See id.* at 333.

30. *See* Waldman, *supra* note 21.

31. 47 U.S.C. § 230(c)(2) (1996).

32. *See* Michelle J. Kane, *Electronic Commerce: Internet Service Provider Liability: Blumenthal v. Drudge,* 14 BERKELEY TECH. L.J. 483 (1999); Waldman, *supra* note 21; Robert T. Langdon, Note, *The Communications Decency Act § 230: Make Sense? Or Nonsense?—A Private Person's Inability to Recover if Defamed in Cyberspace,* 73 ST. JOHN'S L. REV. 829, 848 (1999).

Soon after *Zeran*, *Blumenthal v. Drudge* was decided.[33] In *Blumenthal*, Sidney Blumenthal, a then newly appointed White House aide, sued a gossip columnist and AOL for defamation.[34] The columnist, Mathew Drudge, who was under contract with AOL for his services, posted an article alleging that Mr. Blumenthal was a wife-beater.[35] Though AOL and Drudge later retracted the story,[36] Blumenthal sued both AOL and Drudge.

The United States District Court for the District of Columbia granted summary judgment to AOL citing the immunity provided to ISPs through section 230 of the CDA.[37] Although the court indicated it would have entertained arguments that AOL was a distributor under the common law of defamation, the *Zeran* court's interpretation of section 230 precluded such a hearing.[38] While holding to the precedent that *Zeran* established, the court expressed its frustration with an interpretation of section 230 that allowed AOL to contract for and post Drudge's report, while not facing liability for its falsity.[39]

D. Additional Defamation Issues

1. *Employer Liability for Electronic Defamation by Employees*—It is important to recognize that section 230 only immunizes ISPs.[40] Therefore, the possibility exists that an employer may be liable for an online defamatory statement made by an employee.[41] The *Restatement (Second) of Torts* provides that party

---

33. 992 F. Supp. 44, 46-47 (D.D.C. 1998).
34. *See id.*
35. *See id.* at 46.
36. *See id.* at 48.
37. *See id.* at 49 ("Whether wisely or not, [Congress] made the legislative judgment to effectively immunize providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others.").
38. *See id.* at 51 (concluding that the court in *Zeran* provided a comprehensive interpretation of Section 230's application to ISPs).
39. *See id.* (questioning legislative action that allows an ISP to reap the benefits of a columnist, while escaping all liability for his postings). *See also* Kane, *supra* note 32, at 491.
40. *But see* Michael H. Spencer, *Defamatory E-Mail and Employer Liability: Why Razing Zeran v. American Online is a Good Thing*, 6 RICH. J.L. & TECH. 32 (2000), http://www.richmond.edu/jolt/v6i5/article4.html (last visited May 10, 2001) (proposing that section 230 of the CDA, which immunizes ISPs, defines "interactive computer service" so broadly as to include most employers who provide Internet access to employees) (citing 47 U.S.C. § 230(f)(2) (1996)).
41. Though the CDA offers some immunity to employers, *see* 47 U.S.C. § 223(e)(4) (1996), the immunity does not appear to cover defamatory statements made by employees. For an analysis comparing the CDA's immunities for

A is liable for a defamatory statement posted by party B on land or chattels in A's possession or under A's control if party A was made aware of the defamatory statement and failed to remove the defamatory statement.[42] As the use of company electronic bulletin boards and chat rooms increases, employers in control of these e-forums may need to act quickly to remove any defamatory statement brought to their attentions.[43] In a recently decided case, the New Jersey Supreme Court left open the possibility that Continental Airlines may be liable for defamatory messages posted by its pilots on a frequently used company bulletin board accessible through the Internet.[44] The New Jersey Supreme Court remanded the case to a trial court for a decision on whether the electronic forum was an "integral part of the workplace."[45]

2. *The Publication Element of Defamation and E-mail*—E-mail is another area where employers must be wary because they may be vicariously liable for defamatory e-mail messages sent by their employees.[46] As mentioned earlier, publication is a necessary element of defamation.[47] Because most e-mail messages are instantly copied to another computer or server when sent, these additional copies may constitute a publication. Thus, if employee A writes an e-mail message defaming employee B and sends it only to B, A may be held to have defamed B, who may then seek to hold her employer vicariously liable.[48]

3. *Targeting the "John Doe" Online Critics*—With ISPs largely immune from defamation suits, recent legal disputes have

---

employers and ISPs, see Kaitlin Garvey, Note, *The New Corporate Dilemma: Avoiding Liability in the Age of Internet Technology*, 25 U. DAYTON L. REV. 133 (1999).

42. *See* RESTATEMENT, *supra* note 3, § 577(2).

43. *See* Hellar v. Bianco, 244 P.2d 757, 759 (1952) (allowing a woman to sue a bar owner for failing to remove a defamatory statement about her from the men's room after the bartender was notified).

44. *See* Blakely v. Continental Airlines, Inc. 751 A.2d 538 (N.J. 2000).

45. *See id.* at 551. The Supreme Court's decision did not discuss the CDA. Specifically, the court did not mention any immunity for Continental as an employer under section 223. Further, the court expressed reluctance to hold CompuServe, Continental's ISP, liable, *see id.* at 552, n.11, but did so without finding CompuServe had immunity under section 230 of the CDA.

46. *See* Mia G. Settle-Vinson, *Employer Liability for Messages Sent by Employees via Email and Voice Mail Systems*, 24 T. MARSHALL L. REV. 55, 71 (1998).

47. *See* KEETON ET AL., *supra* note 2 and accompanying text.

48. *Compare* O'Neil, *supra* note 24, at 629-30 (proposing a "presumed publication" rule for online messages), *with* KEETON ET AL., *supra* note 2, at 803 (describing the traditional rule where the defendant is not liable for written statements made about the plaintiff that are sent to the plaintiff in a sealed envelope which is subsequently opened by a third party).

arisen as victims of defamation have sought a more direct approach to stemming the tide of anonymous online bashing of companies.[49] Companies damaged by lies and fictitious stories, often made under the cloak of anonymity provided by Internet chat rooms,[50] have begun to subpoena ISPs for the identities of the anonymous writers.[51] Having the identities of the critics allows the companies to bring defamation suits against the individuals who enjoy no immunity under the CDA.[52] In one case, a company specializing in providing financial education lectures filed a defamation suit, fostering the possibility to subpoena Yahoo!, an ISP, for the identities of ten "John Does" who posted derogatory comments about the company's CEO on one of Yahoo!'s message boards.[53]

More than seventy such lawsuits have been filed around the country in the last few years.[54] To date, ISPs have been complying,[55] which has spawned additional litigation by angry ISP users attempting to keep their identities secret.[56] Online customers who

---

49. *See Company Files Defamation Action against "John Doe" Internet User*, 16 NO. 4 COMPUTER LAW 27 (1999).

50. Such lies or half-truths are known as "cybersmears." *See* David L. Sobel, *The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 VA. J.L. & TECH. 3, at ¶12 (2000). Companies fear that wide dissemination of sensitive or false information over the Internet may even hurt stock prices. *See id.*

51. *See* Carl S. Kaplan, *Judge Says Online Critic has No Right to Hide*, N.Y. TIMES (June 9, 2000), http://www.nytimes.com/library/tech/00/06/cyber/cyberlaw/09law.html (last visited May 10, 2001) (hereinafter *No Right to Hide)*; Carl S. Kaplan, *In Fight over Anonymity, John Doe Starts Slugging*, N.Y. TIMES (June 2, 2000), http://www.nytimes.com/library/tech/00/06/cyber/cyberlaw/02law.html (last visited May 10, 2001); Carl S. Kaplan, *Companies Fight Anonymous Critics with Lawsuits*, N.Y. TIMES (March 12, 2000), http://www.nytimes.com/library/tech/99/03/cyber/cyberlaw/12law.html (last visited May 10, 2001) (hereinafter *Companies Fight*). In the home county of AOL, the sheriff, during a four-month period in 1999, served seventy warrants seeking information from AOL. *See* Sobel, *supra* note 50, ¶ 2, n.1 (citing Stephen Dinan, *Search Warrants Keep AOL Busy*, WASH. TIMES, April 27, 1999, at C4).

52. *See Companies Fight*, *supra* note 51.

53. *See id.*

54. *See No Right to Hide*, *supra* note 51.

55. AOL's policy is to notify the anonymous users of any civil subpoenas and give them fourteen days to try to block the subpoena. *See* Associated Press, *Raytheon Drops Suit Over Internet Chat*, (May 22, 1999), http://www.nytimes.com/library/tech/99/05/biztech/articles/22raytheon.html (last visited May 10, 2001). After that time, if the subpoena is not blocked, AOL turns over the identities to the party seeking them. *See id.* However, Yahoo! has been widely criticized for complying with subpoenas without notifying the users involved. *See* Sobel, *supra* note 50, ¶ 14.

56. Rebecca Fairley Raney, *Judge Rejects Online Critics Effort to Remain Anonymous*, N.Y. TIMES (June 15, 2000), http://www.nytimes.com/library/tech/99/06/cyber/articles/15identity.html (last visited May 10, 2001) (hereinafter *Judge*

have been resisting subpoenas that work to unmask their identities claim that their free speech rights are being compromised.[57] Moreover, others argue that basic notions of fairness and due process are at stake.[58] Nonetheless, in at least some jurisdictions, courts are siding with ISPs that turn over the identities of the alleged defamers to the companies seeking them.[59]

II. Copyright

A. Introduction

Copyright law in the United States is literally as old as the Constitution.[60] In fact, the Constitution provides for the protection of authors' rights "To promote the Progress of . . . useful Arts, by securing for limited Times to Authors . . . the exclusive Right to their respective Writings and Discoveries . . . ."[61]

Today, copyright law is codified by federal statute,[62] which protects "original works of authorship fixed in any tangible medium of expression" including literary, musical, and dramatic works; pantomimes; choreographic works; pictorial, graphic, and sculptural works; motion picture and other audiovisual works; and sound recordings.[63] A fundamental principle of copyright law is that it protects the *expression* of ideas, not the ideas themselves.[64]

Rejects) (A California judge allows a modem company to subpoena Yahoo! for the identity of an online critic concluding that "there is no right to free speech to defame.").

57. *See No Right to Hide*, *supra* note 51 (rejecting First Amendment arguments and ordering Yahoo! and AOL to turn over identities to plaintiff who claims he lost his job based on the defendant "John Doe's" online comments); *see Judge Rejects*, *supra* note 56 (also rejecting defendant's First Amendment arguments).

58. *See* Sobel, *supra* note 50, ¶ 14. Sobel argues further that judicial intervention and subscriber notice of a subpoena is necessary to protect John Doe's rights. *See id.* ¶ 18.

59. *See No Right to Hide*, *supra* note 51 and accompanying text; *see Judge Rejects*, *supra* note 56 and accompanying text. However, Sobel suggests that obtaining the identities of online critics is merely the quickest way to silence them, even without pursuing any further litigation against them. *See* Sobel, *supra* note 50, ¶ 15.

60. U.S. CONST. Art. I, § 8, cl. 8.

61. *See id.*

62. 17 U.S.C. § 101-1332 (1994 and Supp. 1995-2000) (originally enacted as the Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541).

63. *See id.* § 102(a).

64. *See id.* § 102(b) (stating specifically that ideas, processes, procedures and the like cannot, under any circumstances, be copyrighted).

A copyright becomes valid from the moment a work is created and fixed in a medium.[65] A copyright generally remains valid for the life of the author plus seventy years.[66] During this time, no one may reproduce or distribute the work, perform or display the work in public, or prepare derivative works from the copyrighted work without the author's permission.[67]

Because the list of copyrightable works is not fixed, it changes with time and technology.[68] As changes are necessary, the Constitution gives Congress the power to make legislative modifications to protect authors.[69] For example, the Copyright Act has been amended to extend copyright protection to computer programs.[70]

B. Copyright and the Internet

The Internet's speed, wide accessibility, rapid growth, and ability to make exact duplicates of digital files have created copyright issues primarily relating to infringements of an author's *exclusive* right to reproduce his copyrighted works. For example, the Internet allows an individual to distribute a single computer program or other copyrighted work illegally to millions of users, virtually without cost, by merely making it available on a single server and pointing others to that location. Congress has responded to some of the copyright issues raised by the Internet. In 1997 Congress enacted the No Electronic Theft Act (NET Act) in an effort to close a loophole in the Copyright Act which permitted infringers to pirate copyrighted works willfully and knowingly, so long as they did not do so for profit.[71] The NET Act amended

---

65. *See id.* § 102(a). Though not required to create a copyright, it is advisable to include a copyright notice, and to register the work, both of which may be necessary to recover certain damages under the Act. *See* Jeffrey G. Raphelson, *Old Laws, New Laws, and New Technology: A Summary of Some Laws Affecting Use of the Internet*, 77 MICH. B.J. 1202, 1203 (1998).

66. 17 U.S.C. § 302(a) (Supp. 1995-2000).

67. *See id.* § 106.

68. *See id.* § 102(a) (The Act includes language protecting original expressions "now known or later developed.").

69. Sheldon W. Halpren, *Nies Memorial Lecture: Copyright Law in the Digital Age: Malum in Se and Malum in Prohibitum* (Mar. 16, 2000), *in* 4 MARQ. INTELL. PROP. L. REV. 1 (2000) ("What you find if you simply trace the legislation from the late Eighteenth Century to the present is a continuing expansion of the scope of copyright, the scope of copyright owners' rights, and the term of copyright, reflecting some kind of consensus that this kind of protection is needed.").

70. Computer Software Copyright Act, Pub. L. No. 96-517, 94 Stat. 3015, 3028 (1980) (codified as amending 17 U.S.C. §§ 101, 117 (1994 and Supp. 1995-2000)).

71. No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997).

federal copyright law to define "financial gain" to include the receipt of anything of value, including the receipt of other copyrighted works.[72] The NET Act also clarified that when Internet users or any other individuals distribute copyrighted works broadly, even if they did not intend to personally profit, they have violated the Copyright Act. The Act accomplished this by imposing penalties for willfully infringing a copyright: (1) for purposes of commercial advantage or private financial gain, or (2) by reproducing or distributing, including by electronic means, one or more copies of one or more copyrighted works with a total retail value of more than $1,000 during any 180-day period.[73] It also extended the statute of limitations for criminal copyright infringement from three to five years.[74] Moreover, it increased criminal penalties for certain copyright violations:[75] imprisonment may be imposed for up to five years (ten years for subsequent offenses) for willful infringement if the infringer reproduces or distributes at least ten copies or phonorecords with a total retail value of more than $2,500 in a 180-day period.[76]

In 1998 Congress enacted the Digital Millennium Copyright Act ("DMCA"),[77] which amended the Copyright Act to implement the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty of 1996.[78] The WIPO treaty called for adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by copyright owners to prevent unauthorized exercise of their copyrights.[79]

The DMCA contains three principal anticircumvention provisions. The first provision prohibits the act of circumventing a technological protection measure put in place by a copyright owner to control *access* to a copyrighted work.[80] Under the DMCA, "to circumvent a technological measure" means "to descramble a

72. 17 U.S.C. § 101 (Supp. 1995-2000).
73. *Id.* § 506(a).
74. *Id.* §507(a).
75. 18 U.S.C. § 2319 (1994 and Supp. 1995-2000).
76. *Id.*
77. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860, 2887 (1998) (codified as amended in scattered sections of 17 U.S.C.).
78. *WIPO Copyright Treaty*, Article 11, *at* http://www.wipo.int/treaties/ip/copyright.html (last visited Dec. 28, 2001); *WIPO Performances and Phonograms Treaty, at* http://www.wipo.int/treaties/ip/performances/index.html (last visited Dec. 28, 2001).
79. *WIPO Copyright Treaty*, *at* http://www.wipo.int/treaties/ip/copyright.html (last visited Dec. 28, 2001).
80. 17 U.S.C. § 1201(a)(1) (Supp. 1995-2000).

scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[81] The second provision prohibits creating or making available technologies developed or advertised to defeat technological protections against unauthorized *access* to a copyrighted work.[82] The third provision prohibits creating or making available technologies developed or advertised to defeat technological protections against unauthorized *copying* or other infringements of the exclusive rights of the copyright owner.[83] Thus, the first two prohibitions deal with access controls while the third prohibition deals with copy controls. They make it illegal, for example, to create or distribute a computer program that can break the access or copy protection security code on an electronic book or a DVD movie. The Act provides civil remedies including injunctions, damages (actual and statutory), attorneys' fees, and destruction of the offending device.[84] It also imposes criminal penalties of fines or imprisonment or both.[85]

The Digital Theft Deterrence and Copyright Damages Improvement Act of 1999 amended federal copyright law with respect to the statutory damages available for copyright infringement by increasing the minimum damages from $500 to $750 and the maximum damages from $20,000 to $30,000.[86] It also increased the maximum additional damages a court may award for willful infringement from $100,000 to $150,000.[87]

Because an author has the exclusive right to reproduce and display his work, posting a copyrighted work or sending an e-mail containing that work may constitute copyright infringement.[88] It is virtually impossible to view or post anything on the Internet without making a copy of it, at least temporarily in the computer's RAM,[89] on the computer's hard drive, or on a floppy disk.[90] Courts

81. *Id.* § 1201(a)(3)(A).
82. *Id.* § 1201(a)(2).
83. *Id.*§ 1201(b)(1).
84. 17 U.S.C. § 1203 (Supp. 1995-2000).
85. *Id.* § 1204(a).
86. The Digital Theft Deterrence and Copyright Damages Improvement Act of 1999, Pub. L. No. 106-160, 113 Stat. 1774 (1999) (codified as amending 17 U.S.C. § 504(c) (Supp. 1995-2000) to increase statutory damages for copyright infringement).
87. *Id.*
88. *See* Raphelson, *supra* note 65, at 1203.
89. RAM is the acronym for random access memory, which is a common form of computer memory that temporarily stores information for software or web sites as they are used. *See Webopedia at* http://webopedia.internet.com/TERM/R/

have held that even a temporary copy of another person's work made in RAM constitutes copyright infringement.[91] Furthermore, e-mails also fall within the scope of some of these decisions, since any electronic transmission containing the copyrighted work may violate the author's exclusive right to distribute,[92] to perform, or to display the work in public.[93]

The music industry has been the most publicized entity to raise concerns about the electronic distribution of copyrighted works. The emergence of the MP3[94] file format has provided millions of users the opportunity to download compact disc quality music from the Internet. Because these exchanges are usually established

---

RAM.html (last visited May 10, 2001).

90. *See* Fred H. Cate, Note, *Law in Cyberspace*, 39 HOW. L.J. 565, 575 (1996) ("It is simply impossible to read, view, listen to, print, upload, download, transfer, or otherwise access digital expression without making at least one copy of it."). The author makes an interesting comparison between online and hardcopy versions of newspapers. Though the Copyright Act does not protect ideas or facts, the facts and ideas contained in online newspapers are essentially protected because the paper cannot be viewed without making a reproduction. *See id.* at 577. However, the hard copy version of the same newspaper could be shared with a friend without making a reproduction; therefore, allowing the facts and ideas to be viewed without violating the Copyright Act. *See id.*

91. *See* Ian C. Ballon, *Using Trademarks to Drive Traffic to Web Sites and Other E-commerce Law Issues*, 599 PLI/PAT 111, 127-128 (2000) (citing Religious Tech. Ctr. v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. 1361, 1378 (N.D. Cal. 1995) for the proposition that browsing on the Internet creates a copy in RAM that courts have found to be a violation of the Copyright Act); William M. Hart, *An Overview of the Copyright Law*, 599 PLI/PAT 7, 107-09 (2000) (citing MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993) where the court rejected argument that copy in RAM does not infringe because it is not "fixed"). *See also* Raymond Chan, *Internet Framing: Complement or Hijack?*, 5 MICH. TELECOMM. & TECH. L. REV. 143, 165 (1998-1999) (analyzing whether the individual "packets" of information that may be stored in the RAMs of many different computers during an Internet transmission constitute infringements); Allison Roarty, Note, *Link Liability: The Argument for Inline Links and Frames as Infringements of the Copyright Display Right*, 68 FORDHAM L. REV. 1011, 1037 n.222 (1999) (noting that the Digital Millenium Copyright Act of 1998 provides a narrow exception to RAM infringement where computer repairs are being made).

92. *See* Keith Kupferschmid, *Lost in Cyberspace: The Digital Demise of the First-sale Doctrine*, 16 J. MARSHALL J. COMPUTER & INFO. L. 825, 850 (1998) (interpreting the Copyright Act as recognizing that a distribution occurs whenever "a work is transferred from one location to another," or from one computer to another via the Internet).

93. *See* Cate, *supra* note 90, at 576 (concluding that reading a copyrighted work on one's computer constitutes an infringing public display or performance within the Act's definition).

94. MP3 is short for "Motion Picture Experts Group Layer 3 Compression Format," which is the latest file format ideal for digitally storing and copying music. *See* Mary Jane Frisby, Note, *Rockin' Down the Highway: Forging a Path for the Lawful Use of MP3 Digital Music Files*, 33 Ind. L. Rev. 317, 318-19 (1999).

between two computers through the World Wide Web, ISPs became a prime target for liability.[95] Depending on an ISP's intent, knowledge, or control related to the infringing behavior of it users, courts have held ISPs liable for direct, contributory or vicarious infringement.[96] However, Congress essentially immunized ISPs against liability for third-party infringement in the Digital Millennium Copyright Act of 1998.[97] A clear consequence of this Congressional action parallels what occurred after the passage of the CDA's ISP immunizing provisions: the actual "John Doe Infringer" will be targeted.[98]

Although ISPs have effectively been insulated from liability relating to MP3 downloads, the courts have not yet conclusively resolved whether the end user who downloads copyrighted material is liable for copyright infringement.[99] Further, the Audio Home Recording Act of 1992 ("AHRA"),[100] may be too specific to address potential infringement when downloaded files are copied onto a portable device used to play them.[101] In a recent case, the Ninth Circuit Court of Appeals held that hard drives are not covered in the AHRA; therefore, portable devices that store the MP3 files on a hard drive are legal.[102] In the aftermath of that decision, most

95. *See* Wendy M. Pollack, Note, *Tuning in: The Future of Copyright Protection for Online Music in the Digital Millennium*, 68 FORDHAM L. REV. 2445, 2457 (2000).

96. *See id.* at 2457-58 (discussing inconsistent court decisions on ISP copyright infringement liability). *See also Religious Tech. Ctr.*, 907 F. Supp. 1361, at 1361 (denying summary judgment because there was a material issue of fact whether ISP was contributorily liable for providing Internet access to the electronic bulletin board where the plaintiff's copyrighted information was located).

97. Pub. L. No. 105-304, 112 Stat. 2860 (codified at 17 U.S.C. § 512 (Supp. IV 1998)). *See* Pollack, *supra* note 95, at 2466.

98. *See* Pollack, *supra* note 95, at 2467.

99. *See, e.g.*, Halpren, *supra* note 69, at *8 ("The exemption, the immunity, that was built into the Audio Home Recording Act directed to audio visual tape is broad enough so that when you download an MP3 music file from a web site onto your hard disk, you are not committing an act of infringement."); Pollack, *supra* note 95, at 2461-62.

100. Pub. L. No. 102-563, 106 Stat. 4237 (1992) (codified at 17 U.S.C. § 1001-10 (2001)). The recording industry lobbied for the AHRA to limit significantly the copying of CDs by digital audiotape recorders. *See* Pollack, *supra* note 95, at 2461.

101. The recording industry lobbied for the AHRA to limit significantly the copying of CDs by digital audiotape recorders. *See* Pollack, *supra* note 95, at 2461.

102. *See* Recording Indus. Ass'n of America v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1076-81 (9th Cir. 1999) (finding that computer hard drives, which are usually involved in downloading MP3 files, are exempt from the act). The Recording Industry Association of America sued on the basis of alleged violations of the AHRA; it did not sue for alleged copyright infringement. *See* Rebecca J. Hill, Comment, *Pirates of the 21st Century: The Threat and Promise of Digital Audio Technology on the Internet*, 16 COMPUTER & HIGH TECH. L.J. 311, 332-33

commentators now agree that Congress's carefully worded AHRA was too specific to cover the downloading of MP3 files from the Internet.[103]

Web sites dedicated to MP3 distribution have come under fire in federal courts. A number of recording companies and music publishers sued Napster, a web-based company that offered a program that created a user-driven database and search engine to facilitate MP3 downloads.[104] The plaintiffs claimed that Napster was liable for copyright infringement based on contributory infringement and vicarious liability.[105] In support of the plaintiffs' claims, the plaintiffs argued that Napster committed copyright infringement by engaging in or assisting others in copying, distributing, downloading, transmitting, or uploading copyrighted music without the express permission of the copyright owners.[106] On appeal, the court (1) held that Napster was liable for contributory infringement and vicarious liability only to the extent that it was aware that copyrighted works were available on its servers and that it failed to prevent their free exchange and (2) upheld the plaintiffs' right to an injunction against Napster but modified it to conform to these limitations.[107]

The music industry sued the MP3.com company for copyright infringement because MP3.com provided a means for users to download songs in an MP3 format if those users owned the CDs from which the songs came. The court found that the defendant had willfully infringed plaintiffs' copyrights and ordered judgment in the amount of $53,400,000.[108]

1. Linking and Framing—Hyperlinking enables Internet users to move quickly and easily from one web site to another.[109] When a web site is linked to another, a user can click on highlighted text or a graphic which triggers the page displayed to switch to the new "linked" page.[110] Though most web site owners encourage links to their sites because it increases the number of hits, or visitors

(2000).

103. *See, e.g.*, Halpren, *supra* note 69, at *9; Pollack, *supra* note 95, at 2461-62.

104. A&M Records, Inc. v. Napster, Inc., 2001 U.S. App. LEXIS 5446 (9th Cir. 2001).

105. *Id.* at 1011.

106. *Id.*

107. *Id.* at 1021, 1027.

108. UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

109. *See* Roarty, *supra* note 91, at 1014-15.

110. *See id.* (providing a detailed analysis of the different methods used to link).

to their sites, others may not want additional links.[111] Hyperlinking to a file without an owner's permission may be a violation of his exclusive right to display, distribute, or reproduce that file in public.[112]

Framing on the Internet occurs when the information from the linked web site is viewed from within the linking web site.[113] For example, a user on X's web site clicks on a link to Y's web site. Instead of being sent directly to Y's web site, the information is imported into X's web site. This can be misleading as to which web site is providing the linked information because the user views the linked site's information bordered, or framed, by the linking site. Thus, it appears that the linking site is providing the information. In one landmark case, the *Washington Post* sued *Total News* for copyright and trademark infringement after *Total News* continued to frame the *Washington Post*'s articles.[114] When a user on the *Total News* site clicked on the *Washington Post* link, the article appeared, but it remained framed by the *Total News* web site.[115] Thus, it gave the appearance that *Total News* was the source of the information.[116]

A significant case, *Universal City Studios, Inc. v. Reimerdes,*[117] was a 2000 United States District Court for the Southern District of New York case that involved linking. Motion picture studios distribute many of their copyrighted motion pictures for home use on digital versatile disks ("DVDs"), which contain copies of the motion pictures in digital form.[118] They protect those motion

111. *See id.* at 1016.

112. *See* Jeffrey J. Look, *The Virtual Wild, Wild West (WWW): Intellectual Property Issues in Cyberspace—Trademarks, Service Marks, Copyrights, and Domain Names*, 22 U. ARK. LITTLE ROCK L. REV. 49 (1999). However, some argue that the Internet boasts an implied license to link. *See* Robert L. Tucker, *Information Superhighway Robbery: The Tortious Misuse of Links, Frames, Metatags, and Domain Names*, 4 VA. J.L. & TECH. 8, ¶ 37 (1999).

113. *See* Roarty, *supra* note 91, at 1018 (describing in detail the technical aspects of web site framing).

114. No. 97-Civ.-1190 (S.D.N.Y June 5, 1997). *See also* Look, *supra* note 112, at 80.

115. *See* Look, *supra* note 112, at 80.

116. The parties ultimately settled agreeing that Total News could continue linking to the plaintiffs' web sites but could not use framing technology and that Total News had to show that the information was being provided by the Washington Post. *See* Look, *supra* note 112, at 80. *See also* Futuredontics, Inc. v. Applied Anagramics, Inc., 1998 WL 132922 (C.D. Cal. Jan. 30, 1998), *aff'd* 152 F.3d 925 (9th Cir. 1998) (permitting a copyright infringement claim based on framing).

117. 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

118. *Id.* at 303.

pictures by using an encryption system called Content Scramble System ("CSS") that prevents copying.[119] CSS-protected motion pictures on DVDs may be viewed only on players and computer drives equipped with licensed technology that permits the devices to decrypt and play, but not copy, the films. In late 1999, computer hackers devised a computer program called "DeCSS" that circumvented the CSS protection system and allowed CSS-protected motion pictures to be copied and played on devices that lack the licensed decryption technology.[120] Eric Corley and his company, 2600 Enterprises, Inc, quickly posted DeCSS on their Internet web site, thus making it readily available.[121] Eight major United States-based movie studios brought suit under the Digital Millennium Copyright Act ("DMCA"). The movie studios sought to enjoin Eric Corley and his company from publicly posting DeCSS and to prevent them from electronically "linking" their site to others that publicly posted DeCSS. Eric Corley and his company responded with what they termed "electronic civil disobedience": increasing their efforts to link their web site to a large number of other web sites that continued to make DeCSS available.[122]

The court issued an injunction in favor of the motion picture studios, stating:

> In this case, plaintiffs have established by clear and convincing evidence that these defendants linked to sites posting DeCSS, knowing that it was a circumvention device. Indeed, they initially touted it as a way to get free movies, and they later maintained the links to promote the dissemination of the program in an effort to defeat effective judicial relief. They now know that dissemination of DeCSS violates the DMCA. An anti-linking injunction on these facts does no violence to the First Amendment. Nor should it chill the activities of web site operators dealing with different materials, as they may be held liable only on a compelling showing of deliberate evasion of the statute.[123]

2. Fair Use—There are, however, valid defenses to accusations of copyright infringement. The copyright laws are based on balancing an author's rights to protect his work with the public's access to the work.[124] Accordingly, the Copyright Act

119. *Id.*
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.* at 341 (citations omitted).
124. *See* Cate, *supra* note 90, at 574.

provides that the fair use of a copyrighted work for purposes such as comment, criticism, news reporting, research, scholarship, or teaching (including multiple copies for classroom use) is not an infringement of copyright.[125] In determining whether the use of a work in any particular case is fair, the courts consider the following factors: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.[126] In past cases addressing new technologies, the United States Supreme Court has suggested that Congress, not the courts, determine what constitutes fair use.[127]

Some commentators have suggested that copyright law has shifted its focus from penalizing reproducers, who copy for personal use, to punishing the exploiters who seek to benefit commercially.[128] Other groups support the "Copyleft" movement, which seeks to keep new technologies open for all.[129] The Copyleft movement encourages special licenses that allow software to be leased to anyone who agrees not to copyright the software.[130] Users can then freely modify or distribute the leased software so long as it is not made proprietary.[131]

III. Trademark

A. Introduction

Like copyright law, federal law primarily governs trademark law. The Federal Trademark Act (the Lanham Act)[132] recognizes four types of trade symbols or marks. A trademark is a *distinctive* mark, word, letter, number, design, picture, or combination in any arrangement that a person adopts or uses to identify the goods he

125. 17 U.S.C. § 107 (2001); Pollack, *supra* note 95, at 2459.
126. 17 U.S.C. § 107 (2001).
127. *See* Pollack, *supra* note 95, at 2460 (quoting Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984)).
128. *See* Halpren, *supra* note 69, at *10.
129. *See* Teresa Hill, *Fragmenting the Copyleft Movement: The Public Will Not Prevail*, 1999 UTAH L. REV. 797 (1999).
130. *See id.* at 811.
131. *See id.*
132. Pub. L. No. 87-772, 76 Stat. 769 (1962) (codified at 15 U.S.C. §§ 1051-1127 (2001)).

manufactures or sells from those manufactured or sold by others.[133] A service mark is used to identify and distinguish the services of one person from those of others.[134] A certification mark is used in connection with goods or services to certify accuracy, composition, mode of manufacture, origin, quality, or that the work or labor in the goods or services was performed by members of a union or other organization.[135] A collective mark is a distinctive mark or symbol used to indicate either that the producer or provider belongs to a fraternal society, organization, trade association, trade union, or that members of a collective group produced the goods or services.[136]

To be protected by the Lanham Act, a mark must be distinctive enough to clearly identify the origin of goods or services.[137] Notwithstanding, the trademark may not be immoral, deceptive, or scandalous.[138] Trademark infringement occurs when a person without authorization uses an identical or substantially indistinguishable mark that is likely to cause confusion, mistake, or deceipt.[139]

B. The Internet and Trademarks

Trademark issues on the Internet first arose with domain names. A domain name is the technical name for a web site's electronic address on the Internet.[140] The domain name constitutes one of the most important ways a user locates a web site. For example, www.unc.edu, www.sony.com, and www.pepsi.com are domain names. Until recently, registering a domain name was done on a first come, first served basis.[141] This prior custom has brought about a practice called Cybersquatting. Cybersquatting is the

133. 15 U.S.C. § 1127 (2001).
134. *Id.*
135. *Id.*
136. *Id.*
137. 15 U.S.C. § 1052 (2001).
138. *Id.* (providing a complete list of registration restrictions). *See also* Look, *supra* note 112, at 51-56 (describing in greater detail the pitfalls of trade symbol registration, which includes trademarks, service marks, and others covered by the Lanham Act).
139. *See* 15 U.S.C. § 1114 (2001). However, the same words or symbols may be registered for trademarks in different areas of commerce if public confusion is unlikely (e.g., Apple or Delta). *See* Look, *supra* note 112, at 52.
140. *See* Tucker, *supra* note 112, ¶¶ 12-14. Common "top-level" domain names are .COM, .GOV. and .EDU. *See* Look, *supra* note 112, at 51.
141. Until 1999, all domain names were registered by Network Solutions, Inc. *See* Look, *supra* note 112, at 55 n.30. Now more than twenty companies can register domain names. *See id.*

registering of domain names containing trademarks owned by others with the intent to sell the rights to the domain name to the companies who own the trademarks.[142] The legal issue raised by cybersquatting is that registering domain names of established companies may constitute trademark infringement. In a well-known case, *Intermatic, Inc. v. Toeppen*,[143] Dennis Toeppen registered more than 200 domain names including: crateand barrel.com, ussteel.com, and deltaair-lines.com.[144] Intermatic, Inc. had been in existence since 1941 and had registered "Intermatic" as a trademark. Intermatic sued Toeppen for trademark infringement for using the domain name "intermatic.com."[145] Although the court denied Intermatic's summary judgment motion on infringement, it did grant Intermatic's motion for summary judgment on trademark dilution.[146]

In 1999, Congress amended the Lanham Act by passing the Anticybersquatting Consumer Protection Act[147] in response to the increasing number of lawsuits against cybersquatters.[148] The Act allows the owner of a mark to bring a civil suit against any person who, with a bad faith intent to profit from that mark, registers or uses a domain name that, at the time of its registration, (1) is identical or confusingly similar to a distinctive mark; (2) dilutes a famous mark; or (3) is a protected trademark, word, or name.[149] The Act specifies factors a court may consider in determining bad faith intent, but prohibits such a determination if the defendant believed, with reasonable grounds, that the use of the domain name

142. *See id.* at 60.
143. 947 F. Supp. 1227 (N.D. Ill. 1996).
144. *See* Raphelson, *supra* note 65, at 1205.
145. *See id.*
146. *See id.*
147. Pub. L. No. 106-113, 113 Stat. 1501 (1999).
148. *See* Tucker, *supra* note 112, at ¶ 92 (1999) (citing Greg Miller, *Cyber Squatters Give Carl's Jr. Others Net Loss*, L.A. TIMES, July 12, 1996, at A1).
149. 15 U.S.C. § 1125 (2001). *See* Joel Voelzke, *New Cybersquatting Law Gives Trademark Owners Powerful New Weapons Against Domain Name Pirates*, 17 No. 2 COMPUTER LAW 3 (2000).

The Trademark Dilution Act of 1995, which became section 43(c) of the Lanham Act, also made it easier to crack down on cybersquatters. Pub. L. No. 104-98, 109 Stat. 985 (1996). *See* Raphelson, *supra* note 65, at 1205. The Trademark Dilution Act allowed owners of "famous" trademarks to seek injunctions against those whose marks diluted the distinctiveness of their marks. *See id.* Diluting a mark's distinctiveness is possible even where the parties do not compete in the same area of commerce. *See id.* In comparison, proving infringement requires showing that consumers would likely be confused by the new mark, which is not probable when the marks represent businesses in totally different areas of commerce. *See id.*

was fair or otherwise lawful.[150] It authorizes a court to order cancellation of the domain name or its transfer to the owner of the mark. In addition to injunctive relief, it makes available remedies such as recovery of the defendant's profits, actual damages, attorneys' fees and court costs. It also provides for statutory damages in an amount of at least $1,000 and up to $100,000 per domain name, as the court considers just. The Act shields a registrar, registry, or other registration authority from liability for damages for the registration or maintenance of a domain name for another, unless there is a showing of bad faith intent to profit from such registration or maintenance of the domain name registration.[151]

In response to the restrictions of the 1999 Act, cybersquatters have begun to register domain names that are incapable of being registered as trademarks.[152] For example, generic words cannot be registered as trademarks, so cybersquatters have been registering domain names such as www.lawyer.com and www.business.com.[153] Moreover, cybersquatting has spawned a new cottage industry, cyber bounty hunters,[154] who specialize in surfing the net for trademark infringers and cybersquatters.[155]

An alternative way for users to find Internet sites is by using search engines, each of which uses its own algorithm for searching through the Internet and arranging the order of the sites it reports. The operating mechanism of search engines has generated legal issues regarding the use of metatags. Metatags are essentially key words that web site designers and owners use to describe the contents of their sites. These words and phrases are embedded within the HTML document and are not readily visible.[156] Search engines such as Yahoo! and Excite use these metatags to create

150. 15 U.S.C. § 1125 (2001). *See* Joel Voelzke, *New Cybersquatting Law Gives Trademark Owners Powerful New Weapons Against Domain Name Pirates*, 17 No. 2 COMPUTER LAW 3 (2000).

151. *See id.* The Act also allows plaintiffs to file in rem actions against the domain name itself. This provision is especially beneficial when the domain name owner cannot be located, or for whom personal jurisdiction cannot be achieved.

152. *See* Look, *supra* note 112 at 69.

153. *See id.* In addition, the development of new top-level domain names, i.e. .biz, may cause more consumer confusion as identical names registered under .com, could also be registered under .biz. *See id.* at 83. Recently, the addition of new top-level domain names .biz and .info were approved by the Internet Corporation for Assigned Names and Numbers (ICANN). http://www.icann.org /announcements/icann-pr15may01.htm (last visited May 30, 2001).

154. *See* Look, *supra* note 112, at 60.

155. *See id.*

156. *See* Tucker, *supra* note 112, ¶ 70.

large indexes that are scanned for matches when users ask a search engine to find web sites on specific subjects.[157]

Legal controversy has arisen when one web site uses metatags that are actually trademarks of another company in order to divert traffic form the competitor's site to its own site. The practical result is that a user who searches for Brand X may be sent to Brand Y's web site because Brand Y uses Brand X's trademark as a "hidden" metatag. The first such metatag case was *Playboy Enterprises, Inc. v. Calvin Designer Label* where the defendant used "playboy" as a metatag for its site.[158] The court, ruling for Playboy, enjoined Calvin Designer Label from further use of that trademark.[159] Thus, courts have upheld suits alleging trademark infringement or dilution where the purpose of the metatag was to confuse or deceive consumers.[160]

Another type of metatag litigation has involved the banner advertisements often displayed on the web sites of search engines in an attempt to attract a user to the advertiser's site.[161] In a common but controversial Internet advertising practice known as keying, a search engine offers advertisers the ability to display specific banner ads whenever users enter selected search terms, including trademarks or metatags of a competitor's site.[162] For example, Estee Lauder sued Excite for federal trademark infringement after users who typed in trademarked product names of Estee Lauder were presented with banner ads for "The Fragrance Counter."[163] With few court decisions in this area, experts disagree on the likely success of trademark infringement or dilution claims brought by companies against search engines that sell their "keywords" to competitors.[164]

---

157. *See id.*

158. *See id.* ¶ 74 (citing 985 F. Supp. 1220 (N.D. Cal. 1997)).

159. *See* 985 F. Supp. at 1221-22.

160. *See* Tucker, *supra* note 112, ¶ 78. An exception to the use of trademarked metatags may be where a web site sells the trademarked products for that company. *See id.*

161. *See* Matthew A. Kaminer, *The Limitations of Trademark Law in Addressing Trademark Keyword Banners*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 35, 41 (1999).

162. *See id.* at 42.

163. *See id.* at 44 n.52.

164. *Compare*, Kaminer, *supra* note 161, at 45-53 (arguing that the Lanham Act does not prohibit the use of trademarks as triggers for banner ads), *with* Tucker, *supra* note 112, at ¶ 87 (predicting that such unauthorized trademark uses violate at least federal and state dilution laws).

IV. Patents

A. *Introduction*

Patents, unlike copyrights or trademarks, protect ideas and processes.[165] Through a patent, the federal government grants an inventor a monopolistic right to make, use, or sell an invention to the absolute exclusion of others for the life of the patent.[166] To be patentable as a utility patent, the process, machine, manufacture, or composition of matter must meet three criteria: (1) novelty,[167] (2) utility,[168] and (3) non-obviousness.[169] Utility patents have a life that begins on the date of the patent's grant and ends twenty years from the date of the filing of the application.[170] The patent owner may also profit by licensing use the patent to others. The patent may not be renewed and, upon expiration, the invention enters the "public domain." Once in the public domain, anyone may use the patent.

B. *The Internet and Patents*

The explosion of business use of the Internet has necessitated new ways of doing business to adapt to the demands of e-commerce. In the landmark case concerning the validity of patenting such business methods, *State Street Bank & Trust Co. v. Signature Financial Group, Inc,*[171] the court held as patentable a computerized financial system in which individual mutual funds'

165. *See* Raphelson, *supra* note 65, at 1204. However, very much like copyrights, protection for inventors is stated in the Constitution. *See* U.S. CONST. art I, § 8, cl. 8. Also like copyrights and trademarks, patent law is statutory. *See* 35 U.S.C. § 101 (1994).

166. Once a patent has been issued by the Patent and Trademark Office, an inventor has the exclusive rights to make, use and sell his invention. *See* Raphelson, *supra* note 65, at 1204.

167. *See* 35 U.S.C. § 102 (1994).

168. *See id.* § 101.

169. *See id.* § 103.

170. 35 U.S.C. § 154 (1998). Design patents protect "the ornamental aspects of a design or an article of manufacture" for fourteen years from date of issue. *Id.* § 173. Finally, plant patents are issued as either utility or design patents for plants that have been genetically altered in some way. *See id.* Indeed, a key Internet issue of web designs and icons is determining whether one should seek design patent, copyright, or trademark protection. *See* Look, *supra* note 112, at 85-88.

171. 149 F.3d 1368 (Fed. Cir. 1998), *cert. denied*, 525 U.S. 1093 (1999). *See* William D. Wiese, *Death of a Myth: The Patenting of Internet Business Models After State Street Bank*, 4 MARQ. INTELL. PROP. L. REV. 17, 36-37 (2000).

contributions to an investment portfolio are calculated daily.[172] This decision paved the way for other Internet business patents such as: (1) Lycos's Internet search method; (2) Priceline.com's Name-Your-Price Reverse Auctions; and (3) Pitney Bowes's Internet postage delivery system.[173]

According to some commentators, issuing business methods patents will only hurt competition by putting previously widely used technologies out of reach of those companies who cannot afford the licensing fees to use the method.[174] At the same time, allowing business methods patents may permit inept Internet companies to stay in business merely because they own certain patents.[175]

V. Trade Secrets

A trade secret is commercially valuable information that is guarded from disclosure and is not general knowledge.[176] The recipe for making Coca-Cola is a famous example of a trade secret.[177] Generally, state law governs trade secrets providing civil remedies for misappropriation of the trade secrets.[178] Trade secrets are most frequently misappropriated in two ways: (1) an employee wrongfully uses or discloses such secrets or (2) a competitor wrongfully obtains them.

Unlike other areas of intellectual property law, the Internet explosion has created few new issues for trade secret law. It has, however, facilitated the disclosure of trade secrets by disgruntled employees and the theft of trade secrets by competitors.[179]

---

172. *See id.*

173. *See id.* at 27-30.

174. *See* Rochelle Cooper Dreyfuss, *Essay: Are Business Method Patents Bad for Business?*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 263, 270-71, 275 (2000) (based on a speech given at Santa Clara University School of Law); Wiese, *supra* note 171, at 26-27.

175. *See* Dreyfuss, *supra* note 174, at 270.

176. Uniform Trade Secrets Act, § 1. *See* Bruce T. Atkins, Note, *Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. ILL. L. REV. 1151, 1152 (1996); Ryan Lambrecht, Note, *Trade Secrets and the Internet: What Remedies Exist for Disclosure in the Information Age?*, 18 REV. LITIG. 317, 320-23 (1999) (providing the elements of trade secrets recognized by most states).

177. *See* Atkins, *supra* note 176, at 1152.

178. Uniform Trade Secrets Act, §§ 2-4. *See* Lambrecht, *supra* note 176, at 321-23.

179. *See* George J. Moscarino & Michael R. Shumaker, *Changing Times, Changing Crimes: The Criminal's Newest Weapon and the U.S.'s Response*, 16 DICK. J. INT'L. L. 597, 600 (1998) (In 1989, Carnegie-Mellon University's Computer Emergency Response Team received 132 reports of illegal computer entries. *See id.* By 1995, the number of calls received jumped by 1800%. *See id.*).

Congress enacted the Economic Espionage Act of 1996 to prohibit the theft of trade secrets and provide criminal penalties for violations; the statute does not provide any civil remedies.[180] The Act broadly defines theft to include all types of conversion of trade secrets including:

1. stealing, obtaining by fraud, or concealing such information;
2. copying, duplicating, sketching, drawing, photographing, *downloading, uploading*, photo-copying, or mailing such information without authorization; and
3. purchasing or possessing a trade secret with knowledge that it has been stolen.[181]

The Act punishes thefts of trade secrets, as well as attempts and conspiracies to steal secrets, with fines of up to $500,000, imprisonment for up to ten years, or both.[182] Organizations that violate the Act are subject to fines of up to $5 million.[183]

VI. Contracts

A. Introduction

Contract law provides a means of binding parties to an agreement. Contracts are primarily governed by state common law. The sale of personal property is a large part of commercial activity; Article 2 of the Uniform Commercial Code (the Code, or U.C.C.) governs such sales in all states except Louisiana.[184] A sale consists of the passing of title to goods from seller to buyer for a price. A contract for sale of goods includes both a present sale of goods and a contract to sell goods at a future time.

See Atkins, *supra* note 176, at 1169-70 (noting that even constant employee supervision cannot eliminate the risk that a trade secret may be made public on the Internet).

180. ECONOMIC ESPIONAGE ACT OF 1996, Pub. L. No. 104-294, 110 Stat. 3488 (1996) (codified at 18 U.S.C. § 1831 (2001)). *See* Moscarino & Shumaker, *supra* note 179 at 598.

181. 18 U.S.C. 1832 (2001) (emphasis added).

182. *Id.*

183. *Id.*

184. *See* John D. CALAMARI & JOSEPH M. PERILLO, THE LAW OF CONTRACTS § 1.7, at 17-18 (4th ed. 1998). Ultimately, the U.C.C. was passed by every state except Louisiana. *See id.*

B. Problems Applying Contract and Sale Law to E-commerce

As with other areas of law, contract law is lagging behind the technology of the Internet.[185] Electronic consumer transactions on the Internet raise questions about contract authenticity, bargaining power, enforceability, and even the applicability of current U.C.C. provisions.[186] Moreover, questions have arisen whether the U.C.C., common law, or both apply to Internet business transactions and computer software purchases or licenses.[187]

In particular, software transactions did not fall squarely within the U.C.C.'s definition of a "good"[188] or of a "sale." Thus, the stage was set for a line of cases known as the "shrinkwrap cases," in which the main issue was whether the buyer was bound to the seller's terms written on the box or shrinkwrap in which the software was packaged.[189] In deciding these cases, each court either explicitly or implicitly determined that the U.C.C. applied to software transactions.[190] By analogy, the shrinkwrap cases provided

---

185. *See* John Anecki, Comment, *Selling in Cyberspace: Electronic Commerce and the Uniform Commercial Code*, 33 GONZ. L. REV. 395 (1997/1998) (citing HENRY PERRITT, LAW AND THE INFORMATION SUPERHIGHWAY 2 (1996)).

186. *See* Pratik A. Shah, *The Uniform Computer Information Transaction Act*, 15 BERKELEY TECH. L.J. 85 (2000); Jody Storm Gale, Note, *Service Over the "Net": Principles of Contract Law in Conflict*, 49 CASE W. RES. L. REV. 567 (1999); Zachary M. Harrison, Note, *Just Click Here: Article 2B's Failure to Guarantee Adequate Manifestation of Assent in Click-Wrap Contracts*, 8 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 907 (1998). Additionally, the enforceability of bilateral cyberspace contracts may be suspect for a lack of privity. *See* Robert P. Merges, *The End of Friction? Property Rights and Contract in the "Newtonian" World of On-Line Commerce*, 12 BERKELEY TECH L.J. 115, 199-120 (1997). Because the Internet facilitates transactions, it is possible for information rights to be bought and sold regularly, creating a long chain of possession. *See* Merges, *supra*. If one of the links in the chain lacks privity, it may foreclose a potential cause of action for the titleholder at the end. *See* Merges, *supra*.

187. *See* Gale, *supra* note 186, at 570.

188. *See id.* (discussing whether software qualifies as a tangible, movable good). A good is defined, in part, by the U.C.C. as "all things . . . which are movable at the time of . . . contract for sale . . . ." U.C.C. § 2-105(1) (1998). Questions remain as to whether a web page falls within the definition of a good. *See* Gale, *supra* note 186, at 582.

189. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (following the District Court in applying the U.C.C. to software sales and holding that shrinkwrap licenses were enforceable); Step-Saver Data Systems, Inc. v. Wyse Technology, 939 F.2d 91 (3d Cir. 1991) (assuming that software was a good as defined by the U.C.C. and holding that the terms of the box-top license did not become part of the parties' complete and final agreement). *See* Gale, *supra* note 186, at 571-75 (providing a more comprehensive analysis of these and other shrinkwrap cases).

190. *Compare ProCD*, 86 F.3d 1447 (software governed by U.C.C.), *and Step-Saver Data Systems*, 939 F.2d 91 (software governed by U.C.C.), *with* Anecki,

insight into judicial decisions affecting the purchase of software over the Internet. Typically, before such a transaction is consummated, the buyer must click on a button that then displays the terms of the agreement.[191] Usually, the buyer must agree to those terms before the transaction is complete, thereby forming a contract with the company.[192] Thus, these "clickwrap" licenses operate in the same way as their shrinkwrap counterparts.[193]

Another issue highlighted by the shrinkwrap cases was the hybrid nature of Internet transactions. Traditionally, sales were made for either goods or services.[194] Often a transaction involves goods and services, making it difficult to know whether the U.C.C. or common law applies.[195] Transactions involving customized software and the Internet have further confounded the delineation between goods and services.[196]

C. *The Uniform Computer Information Transactions Act (U.C.I.T.A.)*

The dramatic increase in the number and value of Internet transactions coupled with uncertainty about the applicability of the U.C.C. and common law, prompted the National Conference of Commissioners on Uniform State Laws (NCCUSL) to promulgate the Uniform Computer Information Transaction Act ("U.C.I.T.A.") in 1999[197] to provide a comprehensive set of rules for

---

supra note 185, at 399 (stating that it remains unclear whether courts will apply the U.C.C. to software sales).

191. *See* Harrison, *supra* note 186, at 912.

192. *See id.*

193. Both types of licenses threaten consumer rights by limiting warranties and the buyer's rights. *See id.* at 910, 912. Moreover, based on court opinions, the enforceability of clickwrap licenses appears to be very fact specific. *See id.* at 912-13.

194. *See* JOHN D. CALAMARI & JOSEPH M. PERILLO, THE LAW OF CONTRACTS § 1.7, at 17-18 (4th ed. 1998).

195. Courts vary in their methods for analyzing such "mixed" or "hybrid" contracts. For a review of the dominant tests used by courts, *see* Anecki, *supra* note 185, at 399-400.

196. *See* Gale, *supra* note 186, at 577-80. One aspect of the problem is that when the U.C.C. was drafted and later enacted by the states, the U.S. economy was primarily goods-based. *See* Shah, *supra* note 186, at 85. Over the years, the economy has shifted to a service-based system with the Internet providing a good example of the synergy between goods and services. *See id.*

197. *Uniform Computer Information Transaction Act,* http://www.law.upenn.edu/bll/ulc/ucita/ucita200.htm (last visited May 18, 2001). *See* Shah, *supra* note 186, at 85-88. The National Conference of Commissioners on Uniform State Laws ("NCCUSL") in conjunction with the American Law Institute ("ALI") drafted and passed proposed changes to the U.C.C.. *See id.* After this lengthy process, the

computer information transactions. To date, it has been adopted by only two states and introduced in eight other states.[198]

More specifically, Article 2B was conceived in 1995 to address the contracting challenges the Internet and other computer technologies presented.[199] Although the scope of Article 2B had included all information and digital data,[200] because of intense lobbying pressure,[201] U.C.I.T.A. today covers only computer inform-ation transactions.[202] The U.C.I.T.A. defines a "computer information transaction" as "an agreement or the performance of it to create, modify, transfer, or license computer information or informational rights in computer information."[203] This definition would include transfers of computer programs or multimedia products, software and multimedia development contracts, and contracts to obtain information for use in a program or multimedia product.[204] U.C.I.T.A. also governs access contracts, which are contracts to enter the information system of another to obtain

---

changes are then sent to the fifty states to be individually enacted by each state government. *See id.* Recognizing a need to update the 1940's era U.C.C. with language reflecting the technologies of 2000, the NCCUSL and ALI began drafting U.C.C. Article 2B. *See id.* Article 2B, however, faced stiff opposition during the drafting process from government agencies, private industry, and academics alike. *See id.* As a result, in April 1999, ALI pulled out of the drafting process. Just three months later, NCCUSL passed what was once proposed U.C.C. Article 2B as U.C.I.T.A., paving the way for U.C.I.T.A. to go before each of the fifty states for approval. *See id. See also* Linda J. Rusch, *A History and Perspective of Revised Article 2: The Never Ending Saga of a Search for Balance*, 52 SMU L. REV. 1683 (1999) (providing a comprehensive, first-hand account of the process surrounding the proposed U.C.C. revisions. The author served initially as an observer working with the American Bar Association and later as an associate reporter for the Article 2 Drafting Committee.).

198. *See* National Conference of Commissioners on Uniform State Law, *Introduction and Adoptions of Uniform Acts* (last visited May 9, 2001) *at* http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ucita.asp (last visited May 29, 2001).

199. *See* Shah, *supra* note 186, at 86. For a copy of the act, *see* National Conference of Commissioners on Uniform State Laws, *Drafts of Uniform and Model Acts: Official Site at* http://www.law.upenn.edu/bll/ulc/ulc_frame.htm (last visited May 10, 2001).

200. *See* Shah, *supra* note 186, at 88 n.22.

201. *See id.* at 87 n.12 (listing the various private organizations, including the Recording Industry Association of America and the Motion Picture Association of America, Inc., that objected to the scope of Article 2B.).

202. U.C.I.T.A. § 103 (2001). *See id.* at 88 n.22. U.C.I.T.A. was amended in February 2000. *See* National Conference of Commissioners on Uniform State Laws, *Drafts of Uniform and Model Acts: Official Site at* http://www.law.upenn.edu /bll/ulc/ulc_frame.htm (last visited May 10, 2001).

203. U.C.I.T.A. § 102(a)(11) (2001).

204. U.C.I.T.A. § 102, comment 9 (2001).

information or use that information system for specific purposes.[205] In addition, U.C.I.T.A. applies to support and service contracts.[206] Thus, examples of computer information transactions include contracts to acquire software, online access services and content, books and databases on CD-ROM, and non-trivial software elements embedded in goods. U.C.I.T.A. would also apply to storage devices, such as disks and CD's that exist only to hold computer information. U.C.I.T.A. does *not* govern contracts or licenses for the traditional distribution of movies, books, magazines, or newspapers; it would, however, apply to online books, music, and databases.[207] The parties' agree-ment to communicate in digital form does not bring a transaction within a computer information transaction. For example, a contract for an airline ticket is not a computer information transaction because the ticket may be represented in digital form. In this case, the subject matter of the contract is a service: air transportation.[208]

U.C.I.T.A. adapts Article 2 and common law contract provisions to the special needs and nature of computer information trans-actions.[209] U.C.I.T.A. includes provisions dealing with formation, unconscionability, good faith, interpretation, warranties, risk of loss, transfer of contractual rights, financing arrangements, performance, termination and remedies.[210] Most of these provisions are default rules that the parties may change.[211]

Critics of U.C.I.T.A. claim the act has created new issues in its attempts to solve previously nagging ones.[212] For example, under the U.C.C., courts had difficulty determining when a software transaction was complete.[213] However, many argue that the

205. U.C.I.T.A. §§ 102(a)(1), 103, comment 2 (2001).

206. U.C.I.T.A. § 103, comment 2 (2001).

207. *See* Shah, *supra* note 186, at 88-89 (providing further explanation and examples of U.C.I.T.A.'s scope).

208. U.C.I.T.A. § 102, comment 9 (2001).

209. U.C.I.T.A., Prefatory Note.

210. *Id.*

211. Overview of U.C.I.T.A., National Conference of Commissioners on Uniform State Laws, http://www.nccusl.org/uniformact_overview/uniformacts-ovucita .htm. (last visited Aug. 10, 2000).

212. The Attorneys General of twenty-four states wrote a letter to the NCCUSL urging it not to adopt the U.C.I.T.A. until problems they had identified had been addressed, http://www.arl.org/info/frn/copy/agoppltr.html (last visited May 10, 2001); http://www.arl.org/info/frn/copy/agopltr2.html (last visited May 10, 2001). The Bureaus of Consumer Protection and Competition and the Policy Planning Office of the Federal Trade Commission wrote a letter to the NCCUSL expressing a number of concerns when the conference was considering adoption of the U.C.I.T.A.. http://www.ftc.gov/be/v990010.htm (last visited May 10, 2001).

213. Assent may be determined by a traditional offeror/offeree approach or by

U.C.I.T.A. has not remedied the situation because under U.C.I.T.A., assent is too easily manifested and may be recognized even through inaction.[214] Based on these concerns, opponents claim that U.C.I.T.A. jeopardizes a consumer's freedom to contract.[215]

One of the most frequently criticized provisions of the U.C.I.T.A. is its rule permitting shrink-wrapped and clickable contractual provisions to be disclosed *after* the consumer has paid for the software and opens the package. The U.C.I.T.A. permits a mass marketed shrinkwrap license[216] if: (1) the purchaser had reason to know that more terms would be coming; (2) the purchaser is given a right to return the product if he objects to the terms; (3) the right of return is cost-free; and (4) the license does not alter terms to which the parties had actually agreed.[217] The delayed disclosure approach of U.C.I.T.A. applies to all terms, including *warranty disclaimers*, remedy limitations, and restrictions on transfer and use.[218] Permitting the withholding of warranty information until after the sale conflicts with the approach of the Magnuson-Moss Warranty Act.[219]

Perhaps a more troubling issue is the potential for clickwrap agreements to supersede copyright laws. Currently, copyright laws balance an author's rights to reproduce, distribute and display

---

the conduct of the parties. *See* Gale, *supra* note 186, at 581. Either way, shrinkwrap and click-wrap licenses make it difficult to judge assent. *See id.*

214. *See* Shah, *supra* note 186, at 91-93 (claiming that consumers may assent to terms including opt-out clauses, where the U.C.I.T.A. would not apply. The possibilities are high for such confusion because U.C.I.T.A.'s requirement that opt-out clauses be "conspicuous" is not all that stringent.); Gale, *supra* note 186, at 584-585; Harrison, *supra* note 186, at 937-38 (criticizing Article 2B for allowing consumers to consent to agreements on the Internet merely by having had the "opportunity to review" the terms of a license, even if they never did, but began using the information available).

215. *See generally* Gail E. Evans, *Opportunity Costs of Globalizing Information Licenses: Embedding Consumer Rights within the Legislative Framework for Information Contracts*, 10 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 267 (criticizing Article 2B's unfairness to consumers and proposing a transnational approach to licensing practices). *See also* Shah, *supra* note 186, at 93-96 (arguing that U.C.I.T.A. threatens to bind consumers to unwanted waivers of warranties, and choice of forum and law provisions); Gale, *supra* note 186, at 584-586 (predicting that because of burdensome rejection requirements for consumers, vendors will be tempted to ship non-conforming goods, and then bind unsuspecting consumers to mandatory arbitration clauses); Harrison, *supra* note 186, at 942-45 (finding that Article 2B makes it too easy for consumers to assent without thoughtfully committing to the agreement).

216. U.C.I.T.A. §§ 102(a)(44), 102(a)(45) (2001).

217. U.C.I.T.A. § 209 (2001).

218. *Id.*

219. Pub. L. No. 93-637, 88 Stat. 2183 (codified at 15 U.S.C. §§ 2301 – 2312 (2001)).

against the public's interest in enjoying the work.[220] Online licensing agreements have begun to dictate terms regarding a purchaser's right to distribute or copy the information bought.[221] Now, an area traditionally governed by copyright law, may be undermined by online contracts under U.C.I.T.A., thus bypassing federal statutes.[222] Essentially, it has been argued, U.C.I.T.A. encourages an online vendor "to write [its] own copyright law, in other words, to privately legislate its own intellectual property rights."[223] The debate continues as to whether federal copyright laws should preempt such contracts.[224]

D. U.E.T.A. and E-Sign

While U.C.I.T.A. largely addresses software licensing, many questions remained as to the enforceability of contracts made entirely electronically either through the Internet or e-mail because of the writing requirements under contract and sales law (statute of frauds).[225] In response, the NCCUSL promulgated the Uniform Electronic Transactions Act ("U.E.T.A.") in July 1999, which has been adopted by more than thirty states and introduced in most other states.[226] The purpose of the Act is to give full effect to electronic contracts, encourage their widespread use, and develop a uniform legal framework for their implementation.[227] U.E.T.A.

---

220. *See supra* notes 60-131 and accompanying text.

221. *See* Shah, *supra* note 186, at 97.

222. *See* Evans, *supra* note 215, at 289-91 (arguing that such U.C.I.T.A. contracts effectively create monopolies on information); Shah, *supra* note 186, at 97-104.

223. *See* Evans, *supra* note 215, at 290.

224. *See* Shah, *supra* note 186, at 98-102 (comparing the "symbiotic" view where U.C.I.T.A. and copyright law work together against the preemptive view premised on the invocation of the Supremacy Clause of the U.S. Constitution in order to protect existing federal copyright laws).

225. *See generally* R.J. Robertson, Jr., *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787 (1998) (though now dated by the passage of U.E.T.A. in the states and E-SIGN by Congress, this article describes earlier concerns about conducting electronic commerce within a legal framework designed for paper).

226. *See* National Conference of Commissioners on Uniform State Laws, *Introductions and Adoptions of Uniform Acts*, *at* http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp (last visited May 29, 2001). For a copy of the Act, *see* National Conference of Commissioners on Uniform State Laws, *Drafts of Uniform and Model Acts*, http://www.law.upenn.edu/bll/ulc/ulc_frame.htm (last visited May 10, 2001). *See generally* Shea C. Meehan, Comment, *Consumer Protection Law and the Uniform Electronic Transaction Act (U.E.T.A.): Why States Should Adopt U.E.T.A. as Drafted*, 36 IDAHO L. REV. 563 (2000) (discussing the scope and specific provisions of U.E.T.A.).

227. *See* UNIFORM ELECTRONIC TRANSACTIONS ACT § 6, Comment 1 (1999).

protects and enforces electronic signatures and contracts despite the statute of frauds.[228] Section 7 of U.E.T.A. accomplishes this by providing:

(1) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
(2) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
(3) If a law requires a record to be in writing, an electronic record satisfies the law.
(4) If a law requires a signature, an electronic signature satisfies the law.

U.E.T.A. further validates contracts formed by machines functioning as electronic agents for parties to a transaction: "A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements."[229] The Act excludes from its coverage wills, codicils, and testamentary trusts as well as all Articles of the U.C.C. except Articles 2 and 2A.[230]

Congress enacted the Electronic Signatures in Global and National Commerce Act ("E-Sign") in 2000.[231] The Act, which uses language very similar to U.E.T.A.'s language, makes electronic records and signatures valid and enforceable across the United States.[232] The Act defines transactions quite broadly to include the sale, lease, exchange, and licensing of personal property and services, as well as the sale, lease, exchange, or other disposition of any interest in real property.[233] E-Sign defines an electronic record as "a contract or other record created, generated, sent,

228. UNIFORM ELECTRONIC TRANSACTIONS ACT § 7. Based on the Act's definitions of electronic, electronic record, and electronic signature, Internet and e-mail transactions are fully enforceable. *See id.* §§ 2(5)-(8). *See also* Meehan, *supra* note 226, at 567-68.

229. UNIFORM ELECTRONIC TRANSACTIONS ACT § 14.

230. UNIFORM ELECTRONIC TRANSACTIONS ACT § 3. *See also* Meehan, *supra* note 226, at 568-69.

231. Pub. L. No. 106-229, 114 Stat. 164 (2000) (codified at 15 U.S.C. §§ 7001 - 7006 (2001)). The act took effect on October 1, 2000, subject to certain exceptions, pursuant to § 107 of Act regarding the electronic record retention provisions of the Act.

232. *Compare* UNIFORM ELECTRONIC TRANSACTIONS ACT § 7, *with* ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT § 101, 15 U.S.C. § 7001 (2001).

233. ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT § 106(13), 15 U.S.C. § 7006(13) (hereinafter ELECTRONIC SIGNATURE ACT).

communicated, received, or stored by electronic means."[234] It defines an electronic signature as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[235] Like U.E.T.A., E-Sign ensures that Internet and e-mail agreements will not be unenforceable based on the statute of frauds by providing:

1. a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
2. a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.[236]

To protect consumers, E-Sign provides that consumers must *electronically* consent to conducting transactions with electronic records after being informed of the types of hardware and software required.[237] Prior to consent, consumers must also receive a "clear and conspicuous"[238] statement informing consumers of their right to: (1) have the record provided on paper or in non-electronic form; (2) receive paper copies of the electronic record after consenting to electronic records; and (3) withdraw consent to receiving electronic records.[239]

As defined by E-Sign, an electronic agent is a computer program or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response.[240] The Act validates contracts or other records relating to a transaction in or affecting interstate or foreign commerce formed by electronic agents so long as the action of each electronic agent is legally attributable to the person to be bound.[241]

E-Sign specifically excludes certain transactions, including (1) wills, codicils, and testamentary trusts; (2) adoptions, divorces, and other matters of family law; and (3) the Uniform Commercial Code

234. ELECTRONIC SIGNATURES ACT § 106(4), 15 U.S.C. § 7006(4).
235. ELECTRONIC SIGNATURES ACT § 106(5), 15 U.S.C. § 7006(5).
236. ELECTRONIC SIGNATURES ACT § 101(a), 15 U.S.C. § 7001(a).
237. ELECTRONIC SIGNATURES ACT §§ 101(c); 15 U.S.C. § 7001(a)(2), (c).
238. "Clear and conspicuous" is not defined in the Act.
239. For a complete list of consumer's rights under the Act, *see* ELECTRONIC SIGNATURES ACT § 101(a)(2), (c)(1), 15 U.S.C. § 7001(a)(2), (c)(1) (2001).
240. ELECTRONIC SIGNATURES ACT § 106(3), 15 U.S.C. § 7006(3).
241. ELECTRONIC SIGNATURES ACT § 101(h), 15 U.S.C. § 7001(h).

other than sales and leases of goods.[242] It also excludes notices of (1) cancellation or termination of utility services (including water, heat, and power); (2) default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual; (3) the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or (4) recall of a product, or material failure of a product, that risks endangering health or safety.[243]

As evidence of Congress's respect for U.E.T.A. and the states that have made it law, U.E.T.A. is not generally preempted by E-Sign.[244] State laws governing electronic transactions that are not technology neutral, however, are preempted by E-Sign.[245] More than forty states have laws affecting electronic transactions.[246] Some states have adopted laws specifying acceptable technologies.[247]

As technology continues to leap forward, most agree that uniformity among the laws designed to address those challenges is the key to success and stability. With respect to electronic signatures, E-Sign has ensured national recognition of electronic contracts and signatures. However, critics are concerned that the legislation's "technology neutral" position may not relieve the financial and convenience concerns of people doing business with parties using varied technologies for electronic records and signatures.[248]

---

242. ELECTRONIC SIGNATURES ACT § 103(a), 15 U.S.C. § 7003(a).

243. ELECTRONIC SIGNATURES ACT § 103(b), 15 U.S.C. § 7003(b).

244. ELECTRONIC SIGNATURES ACT § 102(a)(1), 15 U.S.C 7002(a)(1).

245. ELECTRONIC SIGNATURES ACT § 102(a)(2)(A)(ii), 15 U.S.C. § 7002(a)(2)(A)(ii).

246. *See* W. Everett Lupton, Comment, *The Digital Signature: Your Identity by the Numbers*, 6 RICH. J.L. & TECH. 10, ¶ 35 (Fall 1999), *available at* http://www.richmond.edu/jolt/v6i2/note2.html (last visited May 10, 2001) (providing a survey of current state laws and the technology behind electronic transactions and security).

247. For example, Utah has passed legislation requiring the use of a specific type of digital (not electronic) signature. *See id.* ¶ 36.

248. *See* Kalama M. Lui-Kwan, *Recent Developments in Digital Signature Legislation and Electronic Commerce*, 14 BERKELEY TECH. L.J. 463, 473-480 (1999). Though written before E-Sign was passed, this article raises questions about the costs of technologically inconsistent laws among the states designed to regulate electronic commerce. Moreover, the article suggests that federal legislation could eliminate such problems by specifying acceptable technologies for electronic signatures and their authentication.

E. Non-Compete Agreements

Employees' covenants not to compete (agreements to refrain from a particular trade, profession, or business) are enforceable if (1) the purpose of the restraint is to protect a property interest of the promisee and (2) the restraint is no more extensive than is reasonably necessary to protect that interest.[249] The reasonableness of the restraint depends on the geographic area the restraint covers, the period for which it is to be effective, and the hardship it imposes on the employee and the public.[250] A benchmark for time in many of these agreements has been one year.[251]

Due to the rapid evolution of business practices in the Internet industry, it has been argued that non-compete agreements for Internet company employees need their own rules. For instance, a period of time that is reasonable for a conventional company might be unreasonable for an Internet company. In *Earthweb, Inc. v. Schlack,*[252] the courts were faced with this issue, and the United States Court of Appeals for the Second Circuit upheld a district court decision striking down a one-year non-compete agreement for an Internet employee because it found the time period too long given the "dynamic nature of [the Internet] industry."[253] Emphasizing its point, the district court then concluded that "[w]hen measured against the IT [information technology] industry in the Internet environment, a one-year hiatus from the workforce is several generations, if not an eternity."[254]

National Business Services, Inc. v. Wright,[255] which was decided a year before *Earthweb,* addressed the geographic scope of an Internet non-compete agreement, upholding a one-year time restriction and a territorial clause that prevented the employee from taking another Internet-related job anywhere in the United States.[256] The court stated: "[t]ransactions involving the Internet,

249. RESTATEMENT (SECOND) OF CONTRACTS § 188(a) (1981). *See* Beverly Garofalo & Mitchell L. Fishberg, *Noncompete Agreements*, NAT'L L.J., Jan. 17, 2000, at B7.

250. RESTATEMENT (SECOND)OF CONTRACTS § 188, comment d (1981).

251. *Id.*, comment g.

252. 71 F. Supp. 2d 299 (S.D.N.Y. 1999), *remanded on other grounds*, 205 F.3d 1322, 2000 WL 232057 (2d Cir., 2000).

253. *Id.* at 313.

254. *Id.* at 316.

255. 2 F. Supp. 2d 701 (E.D. Pa. 1998).

256. *Id.* at 709.

unlike traditional 'sales territory' cases, are not limited by state boundaries."[257]

Some experts in the field are urging companies and their lawyers to rethink their non-compete agreements.[258] Suggestions include: (1) limit the number of people asked to sign a non-compete agreement, which adds credibility to the importance of the measure; (2) shorten time restrictions from one year to three to six months; and (3) demonstrate the agreement's fairness by providing the employee with additional consideration for the time in which the non-compete is honored.[259]

F. Business-to-Business Marketplaces

In an effort to compete and cash in on the profits from the success of online marketplaces, businesses are now joining together to form their own cyber markets.[260] Known as business-to-business ("B2B") marketplaces, these sites, which are typically developed by companies within an industry, allow the companies to trade online for supplies and finished products.[261] B2B sites are being developed by companies in a variety of industries producing everything from cars to planes to meats.[262]

The companies responsible for the sites say the B2Bs will create effective, instantaneous communication allowing for paperless sales without middlemen.[263] In the end, the companies argue

257. *Id.* at 708.

258. *See* Beverly Garofalo & Mitchell L. Fishberg, *Noncompete Agreements*, NAT'L L.J., Jan. 17, 2000, at B7.

259. *See id.*

260. By 2004, some estimates have 17% of business-to-business transactions totaling $2.7 trillion occurring online. *See* Stephanie Stoughton, *Killer Bs Business to Business Exchanges Are the New Buzz in Internet Commerce, Transforming the Marketplace for Parts, Supplies, and Goods. But the Exchanges Could Come Back to Sting Traditional Supply Chains*, BOSTON GLOBE, May 15, 2000, at C6.

261. *See* David Leonhardt, *Business-Exchange Sites Raise Questions for Regulators*, N.Y. TIMES ON THE WEB, http://search1.nytimes.com/search/daily/bin/fastweb?getdoc+cyber-lib+cyber-lib+12084+0+wAAA+B2B (last visited Aug. 10, 2000).

262. *See* Leonhardt, *supra* note 261 (Big Three automakers plan for site Covisint); Stoughton, *supra* note 260 (defense and aerospace contractor's B2B site plans); Brian Sullivan, *Antitrust, Monopoly Fears Haunt B-to-B Exchanges. Web site developed by meat companies latest to face questions of price fixing.*, COMPUTERWORLD, May 22, 2000, at 42 (six major meat companies plan B2B). For a closer look at how the Big Three's site might work, *see* Andrea Foster, *Business-to-Business Alliances Raise Antitrust Concerns*, N.Y.L.J., May 4, 2000, at 5.

263. *See* Leonhardt, *supra* note 261.

that B2Bs will result in cheaper prices for consumers who will benefit from increased competition and lower transaction costs.[264]

However, these B2B sites, many of which are still on the drawing board, have drawn the attention of the Federal Trade Commission ("FTC") and the United States Department of Justice.[265] The FTC is concerned that the B2Bs are closely aligning major companies traditionally in competition with each other.[266] Critics assert B2Bs will expose companies to sensitive pricing information, manufacturing outputs, and inventory numbers of their competitors, raising price-fixing, collusion, and other antitrust issues.[267] Moreover, some worry that B2Bs will operate to exclude some competitors.[268] Recently, Ford announced that the "Big Three" automakers will delay launching their B2Bs as the FTC investigates the antitrust concerns of B2Bs.[269]

To combat these concerns, attorneys are suggesting such solutions as: (1) keep any B2B exchange as independent as possible from the companies participating in it;[270] (2) allow other companies to join;[271] (3) set clear policies against collusion;[272] and (4) use firewalls or encryption to maintain confidential communications between companies.[273]

G. Electronic Cash

Much like the hype surrounding point-of-sale ("POS") transactions in the early 1980s, electronic currencies are not popular

---

264. *See id.* One survey found that companies expect to save nine percent on procurement costs because of Internet based business-to-business exchanges. *See* Greta Steyn, *Internet Procurement Raises Fears of Collusions*, BUS. DAY, May 17, 2000, at 2.

265. *See* Sullivan, *supra* note 262.

266. *See* Leonhardt, *supra* note 261 (citing some that fear B2B exchanges will create de facto cartels).

267. *See* Jeffrey P. Weingart & Jennifer L. Gray, *B2B Internet Marketplaces*, NAT'L L.J., June 26, 2000, at B11.

268. *See id.* In addition, questions remain about taxation, regulation, and registration for international exchanges. *See* Steyn, *supra* note 264.

269. *See* Sullivan, *supra* note 262.

270. *See* Leonhardt, *supra* note 261. For example, the board members for a steel exchange, known as Metalsite, see only aggregate data because the board members also work for the individual companies that own the site. *See id.* Others recommend having the site run by a third party entirely unrelated to the companies participating in the exchange. *See* Sullivan, *supra* note 262.

271. *See* Dan Carney, *E-Exchanges May Keep Trustbusters Busy*, BUS. WK., May 1, 2000, at 52.

272. *See id.*

273. *See* Steyn, *supra* note 264. *See generally* Sullivan, *supra* note 262.

among consumers.[274] Electronic currencies take several different forms,[275] but at their core they would enable online purchases to be made without using credit cards.[276] Upon the full development of electronic currencies, target uses would be for very small value transactions (i.e., less than a few dollars),[277] and web sites that charge a small one-time fee to download files.[278]

The biggest hurdle for these entrepreneurs has not been the legalities or enforceability of such payment systems, but the low demand for electronic currencies. Though technological developments would indicate people are eager for a more convenient and anonymous method of buying goods online, statistics show otherwise.[279] Most people prefer the flexibility that comes with using personal checks.[280] Furthermore, when purchases are made online, consumers feel comfortable paying with credit cards.[281] Consequently, most cyber currency companies are bankrupt, struggling, or focusing the lion's share of their business on other Internet technologies.[282]

---

274. *See* Jane Kaufman Winn, *Clash of the Titans: Regulating the Competition between Established and Emerging Electronic Payment Systems*, 14 BERKELEY TECH. L.J. 675, 688 (1999); Peter Wayner, *Electronic Cash for the Net Fails to Catch On*, N.Y. TIMES ON THE WEB (Nov. 28, 1998) http://search1.nytimes.com/search/daily/bin/fastweb?getdoc+cyber-lib+cyber-lib+1249+15+wAAA+cybercash (last visited Aug. 10, 2000). *But see* John Markoff, *Internet Concern Plans System for Small Online Transactions*, N.Y. TIMES ON THE WEB, (Mar. 8, 1999) *at* http://nytimes.com (last visited Aug. 10, 2000) (citing estimates that electronic cash systems will account for 25% of all Internet purchases by 2002).

275. *See* Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 RUTGERS COMPUTER & TECH. L.J. 1, 29-30 (describing a typical electronic payment transaction); Bryan S. Schultz, *Electronic Money, Internet Commerce and the Right to Financial Privacy: A Call for New Federal Guidelines*, 67 U. CIN. L. REV. 779, 785 (1999) (describing an electronic cash transaction); *see* Winn, *supra* note 274, at 691-701.

276. *See* Perritt, *supra* note 275, at 3-4.

277. *See* Markoff, *supra* 274.

278. *See* Winn, *supra* note 274, at 693 (citing the fact that the demand for pay-per-view web sites has not necessitated the need for electronic cash system).

279. Personal checks remain the most popular among consumers, and their usage continues to increase. *See id.* at 682.

280. *See id.* at 683.

281. *See id.* at 687 (citing the consumer protections and minimal risk associated with credit cards); Wayner, *supra* note 274 (quoting Amazon com which says it will even pay for the $50 deductible not paid by credit card issuers in the event of fraud reported by the consumer). Though trouble may be looming for credit card purchases online, they account for only two percent of card transactions, but for 50% of reported fraud. *See* Winn, *supra* note 274. Those numbers may cause merchants to become more receptive to a different electronic payment system.

282. *See* Winn, *supra* note 274, at 691-94, 698-99; Wayner, *supra* note 274 (finding that even cyber money stalwart Cybercash generates most of its income

Although current Internet transactions are not usually made with electronic currencies, experts believe that e-cash will soon grow in use and popularity.[283] If and when that time arrives, legal issues may arise. For now, consumer privacy, proper authentication, and the risk of forgeries seem to be the areas of greatest concern.[284] With the passage U.E.T.A., U.C.I.T.A. and E-Sign, authentication would seem to be less of an issue, as those measures validated the use of electronic transactions and signatures. Consumer privacy has also received frenzied attention, though little regulation over online financial transactions has been promulgated.[285]

H. Conflict of Laws

A complex issue in "real space," the conflict of laws is even more complicated in cyberspace.[286] Because the Internet is transnational, legitimate arguments can be made that any conflict of laws analysis must be international in scope.[287]

Traditionally, United States courts determined which jurisdiction's substantive law was applicable based on the geographic area where the contract was formed.[288] Later, a test was developed based on the "most significant relationship," which was

---

through technology that protects credit card transactions).

283. *See* Winn, *supra* note 274, at 688 (noting almost two decades after their introduction, debit cards were widely used by consumers at POS locations, such as the grocery store). Looking ahead, companies are working toward providing consumers with a single web site where they can pay their monthly bills, *see* Winn, *supra* note 274, at 699, which may be necessary to force Americans to throw away their checkbooks. *See id.*

284. *See* Perritt, *supra* note 275.

285. *See* Schultz, *supra* note 275 (proposing that new federal regulations must be passed to protect consumer's privacy rights when conducting Internet transactions). *But see* Perritt, *supra* note 275 (addressing the benefit that electronic cash provides anonymous purchasing power after its initial configuration); Winn, *supra* note 274, at 692-93 (noting that Digicash, not bankrupt, was founded on the idea that consumers would flock to an electronic cash system that guaranteed anynonimity). "[C]onsumers are not sufficiently motivated by privacy concerns to create the demand that DigiCash's early promoters expected." *See* Winn, *supra.*

286. *See* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Aristotle G. Mirzaian, *Y2K Who Cares? We Have Bigger Problems: Choice of Law in Electronic Contracts*, 6 RICH. J.L. & TECH. 20 (Winter 1999/2000), *available at* http://www.richmond.edu/jolt/v6i4/article3.html (last visited May 10, 2001); Note, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75 (1996) (hereinafter *Conflicts*).

287. *See* Goldsmith, *supra* note 286.

288. *See* Mirzaian, *supra* note 286, ¶¶ 107-10.

designed to weigh various factors before determining which state's law applied.[289]

The Internet creates problems for either analysis because it is difficult to define: (1) where a transaction is "located" or formed; (2) where its effects are felt; and (3) where the harm actually occurs. Some commentators recommend federal laws to remedy substantive law conflicts within the United States,[290] multinational treaties for transnational conflicts,[291] or a *lex mercatoria*[292] approach for cyberspace contracts similar to the specialized merchant courts established centuries ago. Others, however, suggest that the difficulty of applying current conflict of law frameworks to the Internet is overblown.[293] They suggest that the issues in cyberspace manifest themselves comparably in other areas of law in which the accepted conflict of laws analyses have been successfully applied.[294] Nevertheless, many authorities recommend that the parties to a contract over the Internet write an enforceable choice of law provision into the electronic contract.[295]

VII. Privacy and the Internet

Technology has greatly increased the ability of online companies to collect, store, transfer, and analyze vast quantities of data about consumers who visit their web sites. The Internet's impact on privacy rights has generated considerable public awareness and consumer concern about online privacy. Almost daily, news stories appear detailing the latest Internet privacy problem.[296]

---

289. *See id.* ¶¶ 111-22 (explaining "most significant relationship test and others).

290. *See id.* ¶¶ 62-64.

291. *See id.* ¶¶ 136-39; *Conflicts*, *supra* note 286, at 110-11.

292. Lex Mercatoria is the law of merchants or commercial law. BLACK'S LAW DICTIONARY 923 (7th ed. 1999). *See* Mirzaian, *supra* note 286, ¶¶ 133-35; *Conflicts*, *supra* note 286, at 108-10 (The author also suggests applying admiralty law or choice of law as applied to Antartica.).

293. *See* Goldsmith, *supra* note 286.

294. *See id.*

295. *See* Goldsmith, *supra* note 286, at 1208; Mirzaian, *supra* note 286, ¶¶ 123-24; *Conflicts*, *supra* note 286, 97-102.

296. *See e.g., Failed Dot-Coms May Be Selling Your Privacy Information*, N.Y. TIMES ON THE WEB (July 1, 2000), http://search3.nytimes.com/search/daily/bin/fastweb?getdoc+cyber-lib+cyber-lib+11979+25+wAAA+privacy (last visited Aug. 10, 2000) (reporting that some bankrupt Internet companies allegedly sold personal information about their former customers); Bob Tedeschi, *DoubleClick Reverses on Using Personal Data*, N.Y. TIMES ON THE WEB, Mar. 2, 2000, at B10, http://search3.nytimes.com/search/daily/bin/fastweb?getdoc+cyber-lib+cyber-lib+10234+64+wAAA+privacy (last visited Aug. 18, 2000) (describing DoubleClick's decision not to associate personal information with other "anonymously collected"

While the specific issues are sometimes intricately technical or legal, in general Internet privacy concerns consist of two distinct branches: (1) protection regarding the collection, use, and accuracy of "personal identifiable information"[297] on the Internet; and (2) freedom from unwanted governmental intrusion through the Internet.

A. Protection of Personal Identifiable Information on the Internet

Statistics show that most Internet users fear exploitation of their personal information including their names, phone numbers, home addresses, credit card information, banking information and social security numbers.[298] Though most attention is given to the involuntary means by which personal identifiable information is obtained, Internet users regularly provide such data voluntarily through online purchases, registrations, applications, and surveys.[299] However, even when a person voluntarily provides the information, most companies do not clearly indicate how that data will be used.[300] As a result, some Internet users regularly lie when filling out such questionnaires to avoid the privacy risks.[301]

The public, academics, and regulators consider the involuntary collection of personal information even more troubling. One method of data capture is through the use of "cookies."[302] Under this method, a text file is placed on a user's computer hard drive by

---

Internet data); *Toy Site Sued Over Privacy Concerns*, N.Y. TIMES ON THE WEB (Aug. 4, 2000) (describing a class-action lawsuit alleging that Toys 'R Us Inc. violated its own privacy policy) http://search3.nytimes.com/search/daily/bin/fastweb?getdoc+cyber-lib+cyber-lib+12687+3+wAAA+privacy (last visited Aug. 10, 2000).

297. *See* Jonathan P. Cody, Comment, *Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1185 n.7 (1999).

298. Karl D. Belgum, *Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, ¶ 3 n.4 (1999) (citing statistics from a poll appearing the March 1998 edition of *Business Week* in which 78% of Internet users said they would use the Internet more if their privacy was "guaranteed"), http://www.richmond.edu/jolt/v6i1/belgum.html (last visited May 10, 2001). *But see id.* ¶ 5 (noting that some criticize those polls based on their question construction).

299. *See* Cody, *supra* note 297, at 1186.

300. A 1998 survey by the Federal Trade Commission found that less than 15% of those web sites surveyed had a posted privacy policy which would indicate to an Internet user how the soliciting company plans to synthesize or distribute his personal data. *See* Belgum, *supra* note 298, ¶ 11.

301. *See* Cody, *supra* note 297, at 1186.

302. *See* Belgum, *supra* note 298, ¶ 14 (explaining that cookies can also capture the type of computer and Internet browser used).

the web site visited.[303] That file contains information about the user that is automatically retrieved by the web site and updated each time the user makes subsequent visits.[304] Thus, over time, the web site compiles information about the user's preferences and personal data. In addition, the user's "clickstream"[305] tracks the user as he clicks on pages within the web site and records where the user goes before and after surfing a specific web site.[306] Gradually, the clickstream builds a map of where the user has been and where he is likely to go.[307]

Whether voluntarily or involuntarily, in one study ninety-two percent of surveyed Internet sites collect personal identifiable information.[308] Typically, companies use the data to build a "profile" of their users.[309] These profiles are then frequently sold to advertising companies that focus marketing based on each user's preferences.[310] The companies contend that consumers benefit from the targeted marketing that presents them with goods and services in which they are likely to be interested.[311] On the other hand, many users view such information as their private property and object to its misappropriation.[312] The fundamental regulatory issue

303. *See id.*
304. *See id.*
305. *Id.*
306. *See id.*; *see also* Kimbrelly Keigler, Note & Comment, *Electronic Banking: Security, Privacy and CRA Compliance*, 2 N.C. BANKING INST. 426, 436 (1998) (describing clickstream and cookies).
307. *See* Belgum, *supra* note 298, ¶ 14. Microsoft and Intel came under fire for introducing unique numerical tags which identified each user of that particular software or hardware. *See id.* ¶ 15. These tags, which were unknown to the users, then enabled the companies to track the users throughout the Internet. *See id.*; *see also* Cody, *supra* note 297, at 1185 n.12.
308. *See* Belgum, *supra* note 298, ¶ 11 (citing a Federal Trade Commission 1998 study).
309. *See* Belgum, *supra* note 298, ¶ 8 (explaining that a "profile" denotes the collection, assimilation and categorization processes of a user's personal data). In fact, a cottage industry has developed where companies collecting the data hire outside consultants to store and analyze it. *See* Debra A. Valentine, *Privacy on the Internet: The Evolving Legal Landscape*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 401, 402 (2000); Cody, *supra* note 297, at 1188.
310. *See* Belgum, *supra* note 298, ¶ 16; Cody, *supra* note 297, at 1186-87. *See generally* Keigler, *supra* note 306 (addressing privacy concerns affecting web-based banking and Internet banks).
311. *See* Valentine, *supra* note 309, at 402-03; Cody, *supra* note 297, at 1186-87.
312. *See* Belgum, *supra* note 298, ¶¶ 7 n.11, 9-12 (noting that much of the same personal data can be found in public records, but the threat is that the Internet makes it possible to collect the data much more easily). In addition, there is increasing concern about the accuracy of information collected over the Internet. *See generally* L. Richard Fischer, *Privacy and Accuracy of Personal Information*, 3 N.C. BANKING INST. 11 (1999).

is to find a balance between an individual's right to privacy and commercial access to personal information.[313]

1. Privacy and Intrusion by Private Parties—The United States Constitution does not protect a person's right to privacy with respect to intrusions by private parties.[314] Moreover, the United States has not adopted sweeping, uniform privacy laws.[315] The United States approach is essentially ad hoc, also known as "sectoral."[316]

Instead, privacy rights regulating the conduct of private parties are derived from tort law of the 20th century, although its roots can be traced to an 1890 law review article written by Samuel Warren and Louis Brandeis concluding that there was a "right to be left alone."[317] From there, well-known legal scholar William Prosser determined that courts and legislatures had really been recognizing four distinct privacy torts: (1) appropriation of a person's name or likeness; (2) unreasonable public disclosure of private facts; (3) unreasonable intrusion on the seclusion of another; and (4) unreasonable publicity that places another in a false light in the public eye.[318] These torts were thereafter embraced by the *Restatement (Second) of Torts*[319] and remain the basis for protecting abuse of personal information by non-governmental parties.[320] However, traditional privacy torts offer little protection for a person whose privacy has been compromised on the Internet.[321]

---

313. For a social analysis of the issue, *see* Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1 (1998).

314. *See generally* Maureen S. Dorney, *Privacy and the Internet*, 19 HASTINGS COMM. & ENT. L.J. 635 (1997) (explaining the evolution of privacy law in the United States).

315. *See id.* at 638. No comprehensive federal privacy laws exist despite nearly annual attempts since 1974 to fill the void. *See* Fischer, *supra* note 312, at 20.

316. Dorney, *supra* note 314, at 638-650 (describing potential state and federal privacy laws). For example, the federal government has passed various targeted privacy laws regulating the release of personal information regarding video rentals, credit reports, and cable. *See id.*; *see also* Belgum, *supra* note 298, ¶¶ 24-26 (defining "sectoral" privacy laws as "piecemeal").

317. *See* Cody, *supra* note 297, at 1192 n.37 (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890)); *see also* KEETON ET AL., *supra* note 2, § 117 at 849-50.

318. *See* Belgum, *supra* note 298, ¶ 19; Cody, *supra* note 297, at 1196. *See generally* KEETON, ET AL., *supra* note 2, at 851-69 (discussing the four privacy torts and possible defenses).

319. *See* RESTATEMENT, *supra* note 3, §§ 652A-652E.

320. *See* Belgum, *supra* note 298, ¶ 19.

321. *See* Belgum, *supra* note 298, ¶¶ 19-23 (providing a detailed analysis of the inherent failures of each traditional privacy tort in protecting online users); Cody, *supra* note 297, at 1196 n.67 (rejecting the applicability of privacy torts to Internet

With increasing public and political pressure to address the dearth of available remedies for online privacy invasions, the FTC has recommended that Congress enact legislation that would establish a basic level of privacy protection for consumer-oriented web sites.[322] Under the proposal, consumer-oriented web sites that collect personal identifying information from or about consumers online would be required to comply with four widely accepted fair information practices:

(1) **Notice**—Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it . . . whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.

(2) **Choice**—Web sites would be required to offer consumers choice as to how their personal identifying information is used beyond the use for which the information was provided [such as completing a purchase] . . . .

(3) **Access**—Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies . . . .

(4) **Security**—Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.[323]

---

consumer concerns). *But see* Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357 (2000) (explaining that current United States federal, state and common laws provide adequate protections for online users concerned about privacy). In addition, it should be noted that critics of any regulation point to the availability of "anonymyzing" sites and software that allow consumers to stifle the collection of personal identifiable information. *See* Belgum, *supra* note 298, ¶ 5.

322. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS iii (2000), *available at* http://www.ftc.gov/reports/privacy2000/prvacy2000.pdf (last visited Oct. 26, 2001).

323. *Id.* (citation omitted); *see, e.g.*, Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. REV. 847 (1998); Dorney, *supra* note 314. For a more esoteric analysis of the debate, *see* Belgum, *supra* note 298, which labels the parties debating as the "dossier society pessimists" (those who fear technology will guarantee the collection and storage of huge volumes of information about each person), the "market opportunists" (those in favor of the commercialization of personal information), and the "privacy peacemakers" (those who want to ensure that Internet commerce is not thwarted by those fearful of the privacy issues). *Id.* at 27. In addition, various federal laws regulating, for example, cable and credit

2. Protecting Children—The Communications Decency Act ("CDA") of 1996 was Congress's attempt to protect children from pornography on the Internet.[324] The Act made it a crime to knowingly send "obscene" or "indecent" content via a telecommunications device to anyone under eighteen.[325] The CDA also criminalized the knowing transmittal of "patently offensive" material, as determined by "contemporary community standards," to anyone under eighteen.[326] However, in *Reno v. ACLU*,[327] the Supreme Court struck down much of the CDA as vague and overly broad,[328] holding that the CDA's language, unlike the obscenity test in *Miller v. California*,[329] did not sufficiently limit the CDA's sweep.[330] Noting the CDA's legal contradictions in defining "patently offensive"[331] and that as a matter of law "indecent" expressions are constitutionally protected,[332] the Court concluded that "the CDA effectively suppresses a large amount of speech that

---

miss the mark on Internet privacy. *See* Cody, *supra* note 297, at 1199-200. Most federal privacy laws are aimed at prohibiting or limiting the distribution of personal information, whereas Internet privacy concerns begin with the actual collection of such information. *See id. But see* Dorney, *supra* note 314, at 646 (proposing the Cable Communications Policy Act as model for online Internet privacy legislation). *See generally* Fischer, *supra* note 312 (issues surrounding privacy and web-based Internet banking).

324. The CDA was enacted as Title V of the Telecommunications Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 133, 135; (codified as amended at 47 U.S.C. § 223 (2000)).

325. 47 U.S.C. § 223(a) (2001).

326. *Id.* § 223(d).

327. 521 U.S. 844 (1997).

328. *See id.* at 849 (citing ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996)).

329. 413 U.S. 15 (1973). In *Miller*, the Court adopted the following test for obscene material not provided protection under the First Amendment: "(a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest, (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value." *Id.* at 24 (citations omitted).

330. 521 U.S. at 872-73.

331. *See id.* at 873 (noting that the Government contends courts will be able to limit the scope of "patently offensive" while *Miller* requires a jury to make the determination based on "contemporary community standards"); *see also* Jason Kipness, *Revisiting* Miller *After the Striking of the Communications Decency Act: A Proposed Set of Internet Specific Regulations for Pornography on the Information Superhighway*, 14 SANTA CLARA COMPUTER & HIGH TECH. L.J. 391 (1998) (proposing the need to redefine the *Miller* obscenity test in light of the Internet and questioning the present value of "contemporary community standards" when the Internet is available in almost every town, city and home).

332. *See* 521 U.S. at 874.

adults have a constitutional right to receive and to address to one another."[333]

In 1998, at the behest of the FTC, Congress enacted the Children's Online Privacy Protection Act ("COPPA"), which became effective in April 2000.[334] The purpose of the Act is to protect children under thirteen from commercial websites that collect, store and distribute their personal data.[335] Much like general web sites, those targeting children offered little notice or protection of personal data.[336] In fact, some sites used questionable means to obtain such information from children.[337] Children present easy targets for obvious reasons: their lack of maturity, understanding, and appreciation of the information they provided.[338]

COPPA applies to a web site or online service directed to children as well as to the operator of any web site or online service that has actual knowledge that it is collecting personal information from a child. COPPA protects children by requiring the operator of any web site or online service directed to children "(i) to provide notice on the web site of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and (ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children."[339]

---

333. *See id.*

334. Pub. L. No. 105-277; 12 Stat. 2681 (1998) (codified as 15 U.S.C. §§ 6501 – 6506 (2001)). *See, e.g.*, Laurel Jamtgaard, *Big Bird Meets Big Brother: A Look at the Children's Online Privacy Protection Act*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 385 (2000); Dorothy A. Hertzel, Note, *Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online*, 52 FED. COMM. L.J. 429 (2000). However, some parents are not aware of COPPA. *See* Karen J. Bannan, *Parents Remain Unclear on Online Privacy Law*, N.Y. TIMES ON THE WEB (May 12, 2000), http://search1.nytimes.com/search/daily /bin/fastweb?getdoc+cyber-lib+cyber-lib+11362+2+wAAA+bannan (last visited Aug. 10, 2000).

335. *See* Hertzel, *supra* note 334. *See also* Jamtgaard, *supra* note 334, at 388 (noting that non-profit and personal home pages with "guest books" are excluded from the Act).

336. *See* Hertzel, *supra* note 334, at 436-37 (citing a 1998 FTC study of 212 children's web sites of which eighty-eight percent collected personal data about the children).

337. *See id.* at 435. Some web sites enticed children to provide information during games, contests or through chats with animated characters. *See id.* COPPA now limits the amount of personal information that web sites may solicit from children during games or contests. *See* Jamtgaard, *supra* note 334, at 389.

338. *See* Hertzel, *supra* note 334, at 434.

339. 15 U.S.C. § 6502(b)(1)(a)(i)(ii) (2001). *See* Jamtgaard, *supra* note 334, at 396-98 (detailing the forms of "verifiable parental consent," including fax,

The ACLU and other plaintiffs challenged the constitutionality of a similar Act, the Child Online Protection Act ("COPA"), on First Amendment grounds. COPA was designed to prevent minors from receiving inappropriate information over the Internet. The district court entered a preliminary injunction in favor of the plaintiffs.[340] The United States Court of Appeals for the Third Circuit affirmed the district court's judgment granting a preliminary injunction.[341] The Acting Solicitor General, on behalf of the United States Attorney General, petitioned for a writ of certiorari to review the judgment of the United States Court of Appeals.[342] The United States Supreme Court granted certiorari on May 21, 2001.[343] Subsequently, the Supreme Court heard oral argument on November 28, 2001, but no decision has been handed down as of this writing.

B. Freedom from Unwanted Governmental Intrusion

Like private companies "profiling" users on the Internet, the government can track individual's cyberspace movements and tap into their e-mail and bulletin board postings.[344] For many, this poses an even greater threat to privacy and autonomy.[345] Statistics show people are even fearful of government regulations designed to protect their personal identifiable information from private parties.[346]

However, unlike private companies' activities, the United States Constitution protects an individual's privacy from intrusion by the government.[347] Moreover, in the landmark case *Griswold v.*

---

telephone, credit card, or even a digital certificate).

340. ACLU v. Reno, 31 F. Supp. 2d 473 (E.D. Pa. 1999).

341. ACLU v. Reno, 217 F.3d 162, 166 (3d Cir. 2000) (stating "We will affirm the District Court's grant of a preliminary injunction because we are confident that the ACLU's attack on COPA's constitutionality is likely to succeed on the merits.").

342. Ashcroft v. ACLU, 532 U.S. 1037 (2001).

343. *See id.*

344. *See* Ira Glasser, *The Internet and the Law: Protecting a New Paradigm: Protecting Free Speech and Privacy in the Virtual World of Cyberspace*, 23 NOVA L. REV. 625, 648-49 (1998).

345. *See id.*

346. *See* Belgum, *supra* note 298, ¶ 5 n.8 (citing a study by Direct Marketing Association which found people were wary of government regulation of personal identifiable information over the Internet).

347. *See* Dorney, *supra* note 314 (noting that Americans enjoy such privacy protections despite the word "privacy" not appearing anywhere in the Constitution).

Connecticut,[348] the Supreme Court recognized "zones of privacy" within the "penumbras" of the First, Third, Fourth, Fifth and Ninth Amendments.[349] Later, Congress ensured that the government agencies would not compromise an individual's personal data by enacting the Privacy Act of 1974.[350]

Even with these Constitutional and legislative protections, the United States Supreme Court has recognized areas in which governmental agencies can monitor or "tap" into a person's communications, even from home.[351] Historically, the government used telephone wiretaps to gather evidence of criminal activity.[352] Now the focus is on the government's access to the Internet, e-mail, and other emerging communication technologies.[353]

In particular, the government's crime-fighting tool, "Carnivore" has raised serious privacy concerns. Carnivore is the name given to the FBI's e-mail reviewing software program.[354] The Carnivore system is attached to an Internet Service Provider's network and searches through all of its customers' electronic messages (including e-mail, web addresses and instant messages) looking for the messages of a person suspected of a crime.[355] A major criticism of the system, however, is that only the FBI knows how it works.[356]

---

348. 381 U.S. 479 (1965).

349. *See id.* at 484.

350. Pub. L. No. 93-579; 88 Stat. 1896, (1974) (codified as 5 U.S.C. § 552(a) (2001));. *see* Dorney, *supra* note 314, at 645-46 (noting that government agencies are permitted to gather only personal information that is necessary for that agency's business).

351. *See* Glasser, *supra* note 344 (citing Olmstead v. United States, 277 U.S. 438 (1927) (allowing unrestricted government wire taps) and Katz v. United States, 389 U.S. 347 (1967) (holding that a proper warrant must precede a wire tap).

352. *See id.*; Christopher E. Torkelson, Comment, *The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment*, 25 SETON HALL L. REV. 1142, 1154-55 (1995).

353. *See* Torkelson, *supra* note 352 (analyzing the Clipper Chip technology and its threat to personal privacy).

354. *See Congress Probes F.B.I. E-Mail Snooping Device*, N.Y. TIMES ON THE WEB (July 25, 2000), http://search3.nytimes.com/search/daily/bin/fastweb?Getdoc+cyber-lib+cyber-lib+12447+2+wAAA+Carnivore (last visited Aug. 10, 2000) (highlighting testimony about the software before Congress).

355. *See id.*

356. *See id.*; *Reno Promises Action on Carnivore*, N.Y. TIMES ON THE WEB (Aug 4, 2000), http://search3.nytimes.com/search/daily/bin/fastweb?getdoc+cyber-lib+cyber-lib+12659+5+wAAA+Carnivore (last visited Aug. 10, 2000) (assuring critics that Carnivore's technology will be reviewed by a select number of experts outside the FBI).

Carnivore has also heated up the debate in Washington over privacy in general.[357] The Carnivore controversy has brought to light the disparity between privacy laws applicable to tapping phone communications and those that apply to e-mail.[358] A phone tap requires only a warrant showing probable cause, while an e-mail tap requires clear and convincing evidence that the subject of the proposed tap has committed a crime.[359]

C. *Employee Privacy*

Employees are subject to electronic surveillance to an extent not easily discernible.[360] Concrete statistics on the number of employers who electronically monitor their employees are difficult to achieve because, by its very nature, most electronic surveillance is undisclosed.[361] Increasingly, the monitoring of an employee's e-mail or Internet activities has become an employer's best reconnaissance technique.[362]

The Internet and more advanced computer networks now allow an employer to monitor all of her employees' e-mail, computer files, and Internet activities from a single central computer.[363] For example, an employer using a proxy server[364] can discover whether an employee has visited a specific web site, and the number of times he has done so.[365] In addition, using readily available commercial software, an employer can know what files an employee has downloaded, which chat rooms he has visited, what

---

357. *See* Carl S. Kaplan, *Privacy Plan Likely to Kick Off Debate*, N.Y. TIMES, Aug. 4, 2000, at B10, *available at* http://www.nytimes.com/library/tech/00/08/cyber /cyberlaw /04law.html (last visited May 10, 2001).

358. *See id.*

359. *See id.* (noting that much of the debate turns on whether the Cable TV Communications Act of 1984 applies to cable-based e-mail messages). The FCC may resolve the issue soon. *See id.*

360. *See generally* Patrick Boyd, *Tipping the Balance of Power: Employer Intrusion on Employee Privacy Through Technological Innovation*, 14 ST. JOHN'S J. LEGAL COMMENT. 181 (1999); Rod Dixon, *With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age*, 4 J. TECH. L. & POL'Y 1 (1999); S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825 (1998).

361. *Compare* Dixon, *supra* note 360, ¶ 51, *with* Boyd, *supra* note 360, at 196 (citing very different statistics on employer surveillance of employees). *See also* Dixon, *supra* note 360, ¶ 15 n.41.

362. *See* Wilborn, *supra* note 360, at 836.

363. *See* Dixon, *supra* note 360, ¶ 28.

364. *See id.* (explaining that a proxy server acts as a buffer between an employee's computer and the Internet thereby recording the Internet address of each web site as referenced by an employee).

365. *See id.* ¶ 29.

Internet e-mail he has received, and where he stored that data on his work computer's hard drive.[366] Moreover, technology permits an employer to count the number of keystrokes an employee makes in an hour.[367]

Employers seek to monitor employee's computer activities for a variety of reasons: security concerns, employee efficiency and productivity, misuse of company resources for personal purposes, and uncovering wrongdoing.[368] Because of the *respondeat superior* doctrine, employers clearly have an interest in limiting their liability for employee misconduct committed through the Internet or e-mail, including sexual harassment, defamation, copyright infringement, and discrimination.[369]

As with other areas of privacy law, there is no omnibus federal statute protecting employees from electronic surveillance at work.[370] Even the Electronic Communications Privacy Act of 1986, which was drafted to help control employer surveillance, has fallen well short of expectations because of large loopholes in the law.[371] Further complicating the issue is the public/private distinction with respect to privacy rights.[372] While government employees benefit from greater privacy protections, private employees, who make up the bulk of the workforce, have less legal ground on which to stand. It has been proposed that Congress enact legislation that would: (1) adapt to new technologies; (2) discourage employer action

366. *See id.*

367. *See id.*, ¶ 51 n.140.

368. *See id.*, ¶¶ 32-33; Wilborn, *supra* note 360, at 836-37.

369. *See id.*, ¶¶ 34-36 (noting an employer's interest in safeguarding against trade secret disclosure).

370. *See id.*, ¶ 60 (calling for an end to unwarranted and surreptitious employee monitoring); Wilborn, *supra* note 360 (seeking comprehensive federal legislation that better balances an employee's reasonable expectation of privacy with that of an employer's concern for security and productivity).

371. Pub. L. No. 99-508, 100 Stat. 1872 (1986) (codified as 18 U.S.C. § 1367 (2001)). *See* Boyd, *supra* note 360, at 198; Dorney, *supra* note 314, at 643-44 (noting that while employers generally may not randomly monitor employees, they may use surveillance, including intercepting e-mail messages, incident to business activities or the protection of the employer's rights or property); Wilborn, *supra* note 360, at 839-41 (addressing the exceptions to the Act).

372. *See* Wilborn, *supra* note 360. "Ironically, by failing to impose constitutional privacy notions on private employers, a majority of American employees receive little to no protection for their reasonable expectations of privacy." *Id.* at 874. Wilborn also repeatedly cites the Supreme Court's decision in O'Connor v. Ortega, 480 U.S. 709 (1987) (plurality opinion), where the Court recognized public sector employees' "reasonable expectation of privacy in their place of work." 480 U.S. at 717.

designed to evade or "work around" the law; and (3) consider an employee's reasonable expectation of privacy.[373]

VIII. Securities and the Internet

A security is defined broadly to include stocks, bonds, notes, certificates of interest, and investment contracts.[374] Federal and state laws regulate securities, though state laws vary widely.[375] The federal laws affecting securities are designed to encourage market transactions while: (1) ensuring individual investors receive full disclosure of important facts and (2) protecting individual investors from fraudulent activities.[376]

The Securities Act of 1933[377] and the Securities Exchange Act of 1934[378] are the basis for federal securities law.[379] The Securities and Exchange Commission ("SEC"), created by the 1934 Act, is a quasi-judicial agency responsible for promulgating securities regulations and monitoring market compliance.[380] The 1933 Act, also called the "Truth in Securities Act," prohibits the offer or sale of any security through the use of the mails or any means of interstate commerce unless a registration statement for that security is in effect or the issuer secures an exemption from registration.[381] The purpose of registration is to adequately and accurately disclose financial and other information on which investors may judge the merits of securities.[382] The 1933 Act prohibits fraud in *all* sales of

373. *See* Wilborn, *supra* note 360, at 851-53.

374. *See* section 2(1) of the Securities Act of 1933, 15 U.S.C. § 77(b) (2001); THOMAS LEE HAZEN, THE LAW OF SECURITIES REGULATION § 1.5, at 28-29 (3rd ed. 1996) (citing that the broad definition of securities has been held by courts to include fishing boats, earthworms, and fruit trees). *See also* section 3(10) of the Securities Exchange Act of 1934, 15 U.S.C. § 78(c) (2001).

375. *See* David M. Cielusniak, Note, *You Cannot Fight What You Cannot See: Securities Regulation on the Internet*, 22 FORDHAM INT'L L.J. 612, 622-23 (1998) (noting that the states enacted securities laws before the federal government). State securities laws are commonly referred to as "blue sky laws." *See* HAZEN, *supra* note 374, § 1.2 at 6 (noting that the "blue sky" label can be traced back to Kansas securities laws).

376. *See* Cielusniak, *supra* note 375, at 624.

377. 15 U.S.C. § 77(a)-77(aa).

378. *Id.* § 78(a)-78(mm).

379. *See* Cielusniak, *supra* note 375, at 623-24 (noting that federal securities regulation resulted from the stock market crash of 1929).

380. Before the 1934 Act creating the SEC, the FTC was the agency responsible for overseeing securities laws. *See* HAZEN, *supra* note 374, § 1.2 at 7-8. For a detailed examination of the SEC's structure, policies and authority, *see generally* HAZEN, *supra* note 374.

381. 15 U.S.C. § 77(l).

382. *See* HAZEN, *supra* note 374, § 1.2 at 7.

securities involving interstate commerce or the mails, even if the securities are exempt from the 1933 Act's registration and disclosure requirements.[383] Civil and criminal liability may be imposed for violations of the 1933 Act.[384]

The Securities Exchange Act of 1934 deals mainly with the secondary distribution of securities. The 1934 Act seeks to ensure fair and orderly securities markets by establishing rules for market operations and by prohibiting fraudulent and manipulative practices.[385] It protects holders of all securities listed on national exchanges, as well as holders of equity securities of companies traded over the counter whose corporate assets exceed $1 million and whose equity securities include a class with 500 or more shareholders.[386] Companies must register such securities and are subject to the 1934 Act's periodic reporting requirements, short-swing profits provision, tender offer provisions, and proxy solicitation provisions.[387] In addition, issuers of securities, whether registered under the 1934 Act or not, must comply with the anti-fraud and anti-bribery provisions of the Act.[388]

To realize the benefits of electronic technology,[389] the SEC has provided interpretative guidance for the use of electronic media for the delivery of information required by the federal securities laws, defining *electronic media* to include audiotapes, videotapes, facsimiles, CD-ROM, electronic mail, bulletin boards, Internet web sites, and computer networks.[390] Basically, electronic delivery must provide notice, access, and evidence of delivery comparable to that provided by paper delivery.[391] In addition, the SEC established the

383. 15 U.S.C. § 77(q).
384. 15 U.S.C. § 77(k), (l), (q), (t), (x).
385. *See* HAZEN, *supra* note 374, § 1.2 at 8-9.
386. 15 U.S.C. § 78(l)(g)(1) and Rule 12g-1, 17 C.F.R. § 240.12g-1 (2001).
387. *See* HAZEN, *supra* note 374, § 9.1 at 407.
388. *Id.*
389. *See*, S.E.C., REPORT TO THE CONGRESS: THE IMPACT OF RECENT TECHNOLOGICAL ADVANCES ON THE SECURITIES MARKETS, http://www.sec.gov/news/studies/techrp97.htm (last visited May 10, 2001). *See generally* Neil D. Schwartz, *Wall Street? Where We're Going We Don't Need Wall Street: Do Securities Regulators Stand a Chance in Cyberspace*, 8 FLA. ST. J. TRANSNAT'L L. & POL'Y 79 (1998);. Kenneth W. Brakebill, Note, *The Application of Securities Laws in Cyberspace: Jurisdictional and Regulatory Problems Posed by Internet Securities Transactions*, 18 HASTINGS COMM. & ENT. L.J. 1901 (1996).
390. Use of Electronic Media for Delivery Purposes, Exchange Act Release No. 36,345, Fed. Sec. L. Rep. (CCH) ¶ 3200, at 3129 n.9 (Oct. 6, 1995); Use of Electronic Media, Exchange Act Release No. 42,728, [2000 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 86,304, at 83,374-83,393 (April. 28, 2000).
391. Use of Electronic Media for Delivery Purposes, 60 Fed. Reg. 53,458 (Oct. 13, 1995).

EDGAR (Electronic Data Gathering, Analysis, and Retrieval) computer system, which performs automated collection, validation, indexing, acceptance, and dissemination of reports required to be filed with the SEC.[392] EDGAR's primary purpose is to increase the efficiency and fairness of the securities market for the benefit of investors, corporations, and the economy by speeding up the receipt, acceptance, dissemination, and analysis of corporate information filed with the SEC.[393] After a phase-in period, the SEC now requires all public domestic companies to make their filings on EDGAR, except filings exempted for hardship.[394] EDGAR filings are posted at the SEC's Web site twenty-four hours after the date of filing.

A. Permitted Securities Activities Over the Internet

The rapid spread of the Internet into the sale of securities can be explained by simple economics: unmatched speed, accessibility, and affordability.[395] In addition, Internet access continues to expand with increasing numbers of potential investors.[396] Some issuers are raising capital online by Internet direct public offerings ("DPO"), which are made without a professional underwriter. It is estimated that several hundred DPOs may have been offered.

For public offerings registered under the 1933 Act, the Internet has provided a new means to disclose certain required documents such as a prospectus. The SEC, however, requires electronic delivery to provide notice, access, and evidence of delivery comparable to that provided by paper delivery.[397] Thus, electronic disclosure by way of a company's Internet web site would not satisfy the delivery requirements under the 1933 Act unless the investor has given prior consent to receive electronic delivery by

392. *Id.* at 53,458.
393. *Id.*
394. *Id.*
395. *See* Schwartz, *supra* note 389; Cielusniak, *supra* note 375 (discussing the explosion of the Internet and its affects on and advantages for investors).
396. Schwartz, *supra* note 389, at 80 (citing statistics demonstrating the increased usage of personal computers and the Internet). The author later notes that Internet-based brokerages are also increasing. Approximately 1.3 million investors have such accounts already amid estimates of more than fourteen million such accounts by 2002. *Id.* at 87-88 (citing *On-line Investing Could Hit U.S. $680 Billion*, FIN. POST, Feb. 18, 1998, at 13).
397. Use of Electronic Media for Delivery Purposes, 60 Fed. Reg. 53,458, 53, 460 (Oct. 13, 1995); SEC Interpretation: Use of Electronic Media, [2000 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 86,304, 83,377 (April. 28, 2000).

that web site or the investor has actually accessed the document on the web site.[398]

For some companies, the registration costs of a public offering under the 1933 Act are prohibitive.[399] However, federal law provides certain exemptions,[400] and the Internet has made these exemptions more accessible. Regulation A permits an issuer to offer up to $5 million of securities in any twelve-month period without registration, provided that the issuer files an offering statement with the SEC's regional office prior to the sale of the securities.[401] An offering circular must also be provided to offerees and purchasers.[402] Regulation A sets no restrictions regarding the number or qualifications of investors who may purchase securities under its provisions and permits advertising and general solicitations. In 1995, relying on Regulation A, Spring Street Brewing Company became the first to use the Internet to sell securities.[403]

Private offerings under Regulation D are also exempt from registration under the 1933 Act.[404] General advertising or solicitation, however, is not permitted, and the securities may be purchased by an unlimited number of "accredited investors" and by no more than thirty-five other purchasers.[405] For exempt private offerings, the use of the Internet poses difficult general solicitation issues. Unless there are methods to restrict access solely to investors qualified to participate in a private offering, an online offering under these exemptions likely would violate the general

398. Use of Electronic Media for Delivery Purposes, 60 Fed. Reg. at 53,461.

399. *See* Jonas A. Marson, Comment, *Surfing the Web for Capital: The Regulation of Internet Securities Offerings*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 281, 283 (2000) (addressing the fixed costs associated with registering public securities).

400. *See id.* at 283-89 (discussing the threshold requirements to qualify for exemption and the restrictions imposed under those exemptions).

401. SEC General Rules and Regulations, 17 C.F.R. §§ 230.251-230.263 (2001). *See* Marson, *supra* note 399, at 288-89 (explaining that Regulation A exemptions are available for offerings not greater than $5 million, and permit Internet-based solicitation and advertising). *See also* Cielusniak, *supra* note 375, at 619 (noting that use of federal exemptions such as Regulation A may provide a shield from federal registration requirements, but not individual state laws).

402. 17 C.F.R. § 230.253 (2001).

403. *See* Schwartz, *supra* note 389, at 85 (discussing the SEC's approval of Spring Street's bulletin board trading system, provided certain modifications were made); Cielusniak, *supra* note 375, at 618-19 (explaining that despite Spring Street's Regulation A offering, it had to comply with the laws of 18 different states and the District of Columbia in order to sell the securities).

404. 17 C.F.R. §§ 230.501-.06.

405. *See* Marson, *supra* note 399, at 284-85 (explaining that Rules 505 and 506 of Regulation D forbid solicitations or advertisements regarding the offering).

solicitation restrictions. The SEC has issued letters to clarify how these offerings can be conducted online without violating the general solicitation restrictions. For example, the IPONet received SEC approval for posting notice of an Internet-based, private offering in a password-protected page of its web site accessible only to members who had previously qualified as accredited investors.[406] For registered public offerings, the Internet has provided a new means to disclose certain required documents such as a prospectus.[407] E-mail disclosure is permitted, but electronic disclosure via a web site or bulletin board does not satisfy the requirements of the Securities Act, unless the investor has given prior consent to receive the documents by those means.[408] In addition, the investor must have similar access to the online document as she would have to the equivalent paper version.[409] This does not mean that an electronic document must be immediately viewable online, but only that its retrieval cannot be more burdensome than it would be with the paper version.[410] Finally, a paper version of the document must be available from the issuer in the event that an investor revokes consent, or technical difficulties warrant its issuance.[411]

The Internet has also affected securities regarding the limited offering of securities during the mandatory waiting period after filing for registration.[412] Typically, issuers will travel with their underwriters to various intimate meetings, known in the industry as

406. *See* Schwartz, *supra* note 389, at 85-86; Marson, *supra* note 399, at 284-85 (noting that IPONet would have been in violation of Regulation D's advertising ban had IPONet not designed its web site to "qualify" investors).

407. *See* sources cited *supra* note 389.

408. Use of Electronic Media for Delivery Purposes, 60 Fed Reg. 53,458, 53,460-61 (Oct. 13, 1995); *see* SEC Interpretation: Use of Electronic Media, [2000 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 86,304 (Apr. 28, 2000). *See* Marson, *supra* note 399, at 291 (detailing the specific requirements of electronic disclosure). *But see id.* at 294-95 (explaining that an issuer may receive "tacit" consent from an investor who goes online and accesses documents that are connected by a hyperlink). Further, such hyperlinked electronic documents are treated by the SEC as their paper equivalents mailed in the same envelope: by viewing one, the investor is assumed to have viewed the other. *See id.*

409. Use of Electronic Media for Delivery Purposes, 60 Fed. Reg. at 53,460; *see* SEC Interpretation: Use of Electronic Media, [2000 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 86,304 (Apr. 28, 2000). Marson, *supra* note 399, at 291-93.

410. Marson, *supra* note 399, at 291-93. Finally, documents that must be together, must be accessible by the same means. *Id.* In other words, if special software is needed to download one of the required documents, but not the other, the disclosure requirements may not have been adequately satisfied. *Id.*

411. *Id.* at 293.

412. *See* Jane Kaufman Winn, *Regulating the Use of the Internet in Securities Markets*, 54 BUS. LAW. 443, 447 (1998).

"road shows," with small groups of targeted investors who may be interested in buying the securities after the registration becomes effective.[413] However, in 1998, the SEC approved the use of the Internet to communicate these road shows.[414]

B. Fraudulent Use of the Internet

Offsetting the benefits of the Internet's speed and accessibility is its anonymity, which enables and protects fraudulent activity.[415] Usually, by the time the fraud is uncovered, it is too late for investors to avoid losses: the web site has vanished. In addition, the Internet confers credibility on information;[416] people tend to believe statements seen on the Internet.[417] Consequently, the Internet facilitates fraud by providing access to large numbers of people with little time, effort, or monetary investment. As a result the Internet has expanded the possibilities for securities fraud and created additional challenges for recovery of money defrauded. The SEC is responding to attempts to use the Internet to perpetrate securities fraud through an evolving program of education, surveillance, and litigation.

Fraudulent statements made through the Internet are typically intended to (1) sell worthless or overvalued securities to the public or (2) manipulate the price of securities traded in the secondary market. One example of the first type of Internet securities fraud is perpetrated by creating web sites that appear to be legitimate company web sites but are really non-existent businesses.[418] Many of these fraudulent sites resemble those of major companies and even include hyperlinks to regulatory agencies.[419] An example of the second type of securities fraud is the "pump and dump."[420] First, the defrauder enters an Internet chat room, under an assumed name, and encourages those online to purchase X Company's stock immediately.[421] This is the pump. Then, while the stock price is

413. *See id.* at 448.
414. *See id.*
415. *See* Schwartz, *supra* note 389, at 81; Cielusniak, *supra* note 375, at 626-27.
416. *See* Schwartz, *supra* note 389, at 81-82.
417. *See id.*
418. *See* Will Morrow, Comment, *Is the Internet Participating in Securities Fraud?: Harsh Realities in the Public Domain*, 72 TULANE L. REV. 2203, 2207-08 (1998); Marson, *supra* note 399, at 630 (noting that many of the well-worn telemarketing scams can also be found online).
419. *See* Marson, *supra* note 399, at 630.
420. Morrow, *supra* note 418, at 2209. *See* Marson, *supra* note 399, at 630-32.
421. *See* Marson, *supra* note 399, at 630-32.

artificially inflated, the defrauder sells his stock for a healthy profit.[422] This is the dump.

C. *Proposed Changes*

The SEC has proposed sweeping changes to existing securities laws.[423] The most well known change is the Aircraft Carrier Release, so named for its very broad proposals, which would alter Internet securities trading in several key ways.[424] First investors would be required to list their e-mail and web addresses on registration documents filed with the SEC.[425] Second, the Aircraft Carrier Release proposes to waive any waiting periods.[426] This would effectively open up electronic road shows to anyone, while at the same time easing fears that hyperlinked web sites might appear to be advertisements rather than informational.[427]

Meanwhile, several states have passed their own Internet securities sales legislation.[428] Experts are divided on the best method for regulating Internet securities. Some favor a strong International approach that would provide clarity to inherent jurisdictional issues,[429] while others have called for a stronger SEC voice, domestically.[430]

IX. Cyber Crime

Defining "cyber crime" or "computer crime" is elusive.[431] For many, cyber crime is any crime committed or facilitated by a computer, such as murder-for-hire over the Internet.[432] But for others, cyber crime describes a new genre of crime that is typically associated with expert computer hackers.[433] However, most agree

422. *See id.*
423. *See* Marson, *supra* note 399, at 298.
424. Proposed Rule: The Regulation of Securities Offerings, Release No. 33-7606A, 63 Fed. Reg. 67,174 (November, 13,1998). *See* Marson, *supra* note 399, at 298. (noting that the Aircraft Carrier Release was heavily influenced by technological advances).
425. *See id.* at 303.
426. *See id.*
427. *See id.* at 303-08.
428. *See* Cielusniak, *supra* note 375, at 636-37.
429. *See* Schwartz, *supra* note 389.
430. *See* Marson, *supra* note 399.
431. *See* Michael Hatcher et al., *Computer Crimes*, 36 AM. CRIM. L. REV. 397, 398-99 (1999); Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 180 (2000).
432. *See* Hatcher et al., *supra* note 431, at 398-99; Sinrod, *supra* note 431, at 180.
433. *See* Hatcher et al., *supra* note 431, at 398-99. A hacker is a person who

that computer crimes are best categorized, at least for purposes of prosecution, based on whether the computer was the target or the instrument of the crime.[434] Determining the role that a computer plays in any crime may be the key to determining which laws have been broken.[435]

Not surprisingly, the proliferation of personal computers and Internet accessibility has fueled a rise in cyber crime. A recent cyber crime study found that more than half of the corporations responding reported unauthorized access of their computers.[436] Of those, sixty-six percent claimed losses of more than $50,000, and eighteen percent claimed losses in excess of $1 million.[437] Further, studies show that computer hackers[438] and online fraud have hit financial institutions especially hard.[439] Even larger is the number of cyber crime related losses that go unreported because the attack was never detected, or because of fears that "hacking" reports might alarm investors or customers.[440]

Examples of cyber crimes using the computer as the instrument include the distribution of child pornography, money laundering and illegal gambling, copyright infringement, the illegal communication of trade secrets, and fraud involving credit cards, e-commerce, and securities.[441] Cyber crime, with computers as a

---

gains unauthorized access to a computer. *Id.* More specifically, a hacker with criminal intent is referred to as a "cracker." *See* Sinrod, *supra* note 431, at 182-83. *See also* Hatcher et al., *supra* note 431, at 400 n.11. Finally, a split has occurred among hackers. *See* Sinrod, *supra* note 431, at 203-04. "Old school" hackers, who apparently adhere to certain ethical hacking standards, complain that the typically teenaged "new school" hackers have diminished the trade and increased awareness resulting in the promulgation of many anti-hacking statutes. *See* Sinrod, *supra* note 431 at 203-04.

434. *See* Hatcher et al., *supra* note 431, at 401 (categorizing crimes based on whether the computer was the object, subject or instrument of the crime); Sinrod, *supra* note 431, at 187-89 (delineating among computers which are targets, tools or incidental to the offense).

435. *See generally* Sinrod, *supra* note 431.

436. *See* Marc S. Friedman & Kristin Bissinger (presented by Mary J. Hildebrand), *"Infojacking": Crimes on the Information Superhighway*, 507 PLI/PAT 1107, 1109-10 (1998) (citing a study by WarRoom Research).

437. *See id.*

438. Estimates put the number of hackers at 100,000, with anywhere from 250 to 1,000 of the most elite being able to pierce most corporate security. *See* Sinrod, *supra* note 431, at 182-83.

439. *See id.* at 1124 (noting that in 1995 Citibank lost $400,000 and nearly $9.6 million more to Russian hackers).

440. *See* Hatcher et al., *supra* note 431, at 399.

441. *See* Friedman & Bissinger, *supra* note 436, at 1110; Sinrod, *supra* note 431, at 178-79. It has been estimated that individuals may lose more than $100 million to Internet fraud each year. *See* Cielusniak, *supra* note 375, at 627.

target, attacks a computer's confidentiality, integrity, or availability; examples include theft or destruction of proprietary information, vandalism, denial of service, web site defacing and interference, and malicious code.[442] This type of crime targets a computer system, generally to acquire information stored on that computer system, to control the target system without authorization or payment, or to alter the integrity of data or interfere with the availability of the computer or server. For example, a hacker might gain access to a hotel reservation system to steal credit card numbers. Or a hacker may seek private information about another individual to extort money or to obtain commercial advantage.

In the category of attacks known as "denial of service," the objective is to disable the target system without necessarily gaining access to it. For example, a common denial of service crime occurs when an Internet Service Provider's central computer, or server, is intentionally flooded with e-mails ("mail bombings") that "bring it down," or freeze it.[443] As a result, customers using the ISP cannot gain access to the Internet and are thus denied service. Web site defacing involves hackers who demonstrate their prowess by illegally substituting their own graphics or language for what is usually seen on a particular site.[444] In addition, some hackers may use the access to a web site as a vehicle to hack further into a company's computer system where they can steal sensitive passwords, alter web sites, copy credit card numbers, plant damaging programs, and create "back doors" which would allow the hacker to re-enter the system at a later date. Finally, hackers plant malicious codes, such as viruses, worms, logic bombs, or Trojan horses, which infect a computer and cause damage to it without the user realizing until it is too late.[445] The irony is that often the user is responsible for launching the virus, usually by opening an e-mail message with an attachment.[446] Worms can cause as much damage as viruses, but

442. *See generally* Sinrod, *supra* note 431.

443. *See id.* at 189-97 (describing at length the many techniques that hackers use to accomplish a denial of service attack).

444. *See id.* at 203-15 (detailing the technical methods hackers use to attack via web sites).

445. *See id.* Some hackers' aim is to gain "root access," also known as the "god account." *See id.* at 205. Having root access essentially means a person has control over the "brain" of the computer system. At that level, hackers can steal sensitive passwords, alter web sites, copy credit card numbers, plant damaging programs and create "back doors" which would allow the hacker to re-enter the system at a later date. *See id.*

446. *See* Sinrod, *supra* note 431, at 218-19 (discussing the 1999 Melissa Virus, launched when an e-mail attachment was opened, which caused as much as $80 million in damages).

can launch without attaching to any other file.[447] Logic bombs are triggered by an event, or a specific time or date.[448] Lastly, Trojan horses are programs that look innocent, but behind the scenes carry on destructive practices.[449]

Increasingly, prosecutors have more and better tools to bring these criminals to justice.[450] Today, every state has laws targeting cyber-criminals.[451] Originally passed in 1984,[452] and amended in 1986, 1994, and 1996, the Computer Fraud and Abuse Act protects a broad range of computers that facilitate interstate and international commerce and communications. The Act makes it a crime with respect any computer that is used in interstate commerce or communications (1) to access or damage it, without authorization; (2) to access it with the intent to commit fraud; (3) to traffic in passwords for it; and (4) to threaten to cause damage to it with the intent to extort money or anything of value.[453] Furthermore, depending on the details of the crime, cyber criminals may also be prosecuted under other federal laws, such as copyright, mail fraud, or wire fraud laws.

447. *See* Sinrod, *supra* note 431, at 221. The most famous worm was developed in 1988 by a graduate student at Cornell University who wanted to expose the security flaws in university and government computers. *See* Friedman & Bissinger, *supra* note 436, at 1113-14; Sinrod, *supra* note 431, at 222. Though Robert Morris never intended his "worm" to cause the extensive national damage it did, he was sentenced to three years probation, 400 hours of community service and $10,500 in fines. *See* Friedman & Bissinger, *supra* note 436, 1114.

448. *See* Hatcher et al., *supra* note 431, at 401 n.18 (noting that while used by hackers for destructive means, logic bombs have been employed by software companies protecting against copyright infringement).

449. *See* Hatcher et al., *supra* note 431, at 401 n.17; Sinrod, *supra* note 431, at 223.

450. The Department of Justice and the FBI each have units dedicated to Cyber-crimes. *See* Friedman & Bissinger, *supra* note 436, at 1132. The FBI has a computer crime team all 56 field offices. *See* Hatcher et al., *supra* note 431, at 420-21 (noting that the FBI has focused attention on fighting the proliferation and distribution of online child pornography). In addition, since 1998 the Justice Department, Defense Department and FBI have been collaborating with private industry to form the National Infrastructure Protection Center which is dedicated to enforcing existing computer laws and investigating future threats. *See* Hatcher et al., *supra* note 431, at 422.

451. *See* Hatcher et al., *supra* note 431, at 425-27. The author noted that at the time of publication Vermont was the only state not to have passed computer crime legislation. *See id.* at 425. Since that time Vermont has enacted a computer crime law. *See* VT. STAT. ANN. tit. 13, §§ 4101-07 (1999).

452. Pub. L. No. 98-473, 98 Stat. 2190 (1984).

453. 18 U.S.C. § 1030 (2001). *See* Sinrod, *supra* note 431, at 226-29.

X. Conclusion

This article covered the areas of the law that have been most significantly affected by e-commerce and the evolution of the Internet: defamation, intellectual property, contract and sales law, privacy, securities regulation, and cyber crime. This article also identified the most significant types of legal and regulatory issues that have arisen or are likely to arise. This article described the extent to which the law has responded or is in the process of responding. Consequently, this article will help business people and lawyers better deal with the considerable uncertainty and numerous opportunities for abuse in cyberspace.

***